Google Inc. et al v. Egger et al
Doc. 469

Exhibit 1

Dockets.Justia.com

Calendar No. 453

110TH CONGRESS, 1st Session | SENATE | REPORT 110–209

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2007

OCTOBER 26, 2007.—Ordered to be printed

Mr. ROCKEFELLER, from the Select Committee on Intelligence, submitted the following

REPORT

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 2248]

The Select Committee on Intelligence, having considered an original bill (S. 2248) to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act and for other purposes, reports favorably thereon and recommends that the bill do pass.

BACKGROUND AND NEED FOR LEGISLATION

The Committee, since its inception in 1976, has exercised sustained oversight of the Executive branch's use of electronic surveillance for foreign intelligence purposes. A central focus of that oversight has been the implementation of the Foreign Intelligence Surveillance Act of 1978 ("FISA") by the Executive branch and by the special court established by Congress to provide judicial oversight of FISA, the Foreign Intelligence Surveillance Court ("FISA Court").

Since the President's acknowledgement of the existence of a presidential program on December 17, 2005, which has been publicly described as the Terrorist Surveillance Program, the Committee has sought to inquire vigorously into the President's authorization for the National Security Agency ("NSA") to conduct electronic surveillance within the United States without FISA court orders. In the past year, the ability of the full Committee to perform the Com-

69–010

mittee's oversight responsibilities has been significantly augmented by improved access to information about the program, as well as information about the shift of activities under that presidential authorization to activities in accordance with orders of the FISA Court.

The Committee has also carefully reviewed the impact of technological change on FISA collection to assess whether amendments to FISA should be enacted. On March 23, 2007, the Chairman and Vice Chairman notified the Attorney General of their intention to focus on whether FISA should be modernized and whether legislation should be enacted to address legal consequences arising from the Terrorist Surveillance Program. The Chairman and Vice Chairman also gave notice of their intention to establish a public record on the question of FISA modernization and requested that the Administration submit a formal legislative request addressing the intelligence challenges arising under FISA in a manner consistent with the Constitution. The Director of National Intelligence ("DNI") submitted a proposal on April 12, 2007.

The Committee received the cooperation of many officials from the intelligence community and the Department of Justice in its oversight activities. The Committee held seven hearings in 2007 on the issues, received many classified briefings, propounded and received answers to many written questions, and conducted extensive interviews with several attorneys in the Executive branch who were involved in the review of the President's program. In addition, the Committee received formal testimony from companies alleged to have participated in the program and reviewed correspondence that was provided to private sector entities concerning the President's program. The Committee secured Inspector General reports and the orders and opinions issued by the FISA Court following the shift of activities to the judicial supervision of the FISA Court. The Committee invited statements from experts on national security law and civil liberties and Committee staff met periodically with them. The Committee has also examined the extensive testimony given before other committees in the last several years.

In one particular respect, the Committee's effort to secure information pertaining to the program was more difficult than it should have been. The Committee repeatedly requested to see the text of the presidential authorizations for intelligence collection outside of FISA and the legal opinions of the Department of Justice that supported those authorizations. Although the Committee had been learning about the substance of these documents from witnesses, seeing the actual text was important for obtaining a complete understanding of the program. These documents were only made available to the Committee for the first time on October 9, 2007. The Committee believes it has been given access to all of the authorizations and opinions it requested; however, its study of these documents will continue following the filing of this report.

Based on its inquiry, the Committee has concluded that: (1) the Protect America Act, enacted in early August, should be revised; (2) FISA should be amended to provide an additional procedure to facilitate the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information; (3) additional protections should be afforded to U.S. persons whose communications are targeted for collection or collected incidentally;

and (4) narrowly circumscribed civil immunity should be afforded to companies that may have participated in the President's program based on written requests or directives that asserted the program was determined to be lawful.

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Created, in part, in response to the surveillance abuses documented by the hearings in the mid 1970s of the Church and Pike Committees, the Committee helped write the Foreign Intelligence Surveillance Act of 1978. FISA, supported by President Ford and signed into law by President Carter, established an independent court to oversee and authorize electronic surveillance as defined in the statute, special procedures for the Executive branch to act in emergencies and wartime, and reporting requirements to the Congress.

FISA offered the Executive branch the certainty of a legal framework, and the affirmation of the Congress, for its intelligence collection activities. While the Supreme Court had expressly declined to address the issues related to surveillance of foreign powers and agents of a foreign power in its landmark 1972 decision known as the Keith case, the Court had held that Section 2511(3) of the Omnibus Crime Control and Safe Streets Act did not constitute a grant of power to the President with respect to national security surveillances and that electronic surveillance in domestic security matters requires an appropriate prior warrant procedure. *See United States* v. *United States District Court,* 407 U.S. 297 (1972). Whatever the reasonable exercise of presidential power to protect national security may have been in the 1970s, the enactment of FISA clarified the validity of the use of information collected under the statute as evidence in subsequent court proceedings. The Act ensured that telecommunication carriers that responded to a FISA court order were given statutory protection against civil liability. Most importantly, the Act represented a balancing by two branches of the government of the security and civil liberties of the American people. As President Carter noted in his signing statement: "It provides a basis for the trust of the American people in the fact that the activities of their intelligence agencies are both effective and lawful."

The FISA process has assisted the Government in securing valuable intelligence over almost 30 years. To ensure that it continues to do so, the statute has been amended many times with the assistance of the Committee to address changing threats, technological challenges, and problems in its implementation. In 1994, for example, FISA was amended to cover physical searches conducted for foreign intelligence purposes. After the terrorist attacks of September 11, 2001, in the USA PATRIOT Act, Congress amended FISA, among other things, to enhance communication and coordination between law enforcement and intelligence personnel, authorize roving wiretaps for foreign intelligence collection, and expand the range of business records that could be obtained with a FISA order. In other measures since the September 11th attacks, the Administration has sought, and the Congress has passed, amendments to FISA to assist the Government in its efforts to detect and prevent terrorist attacks.

THE PRESIDENT'S PROGRAM

In December 2005, the American people, and almost all of the Congress, learned for the first time that, shortly after September 11, 2001, President Bush had authorized the NSA to conduct surveillance activities in the United States to protect the country from future terrorist attacks. The NSA program was described by the Department of Justice in January 2006 as "an early warning system . . . to detect and prevent the next terrorist attack . . . a program with a military nature that requires speed and agility."

After the attacks of September 11, 2001, Congress passed a joint resolution on September 14, 2001, declaring that the attacks "continue to pose an unusual and extraordinary threat" to the country and calling on the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any further acts of international terrorism against the United States . . . .". Authorization for Use of Military Force, Pub. L. No. 107–40, section 2(a), 115 Stat. 224 (2001). The President also declared a national emergency on September 14, 2001, stating that there was "a continuing and immediate threat of further attacks on the United States." The intelligence community assessed in October 2001 that additional waves of al Qaeda attacks were imminent. This assessment was manifested in the mobilization of 35,000 reservists and National Guard troops for homeland defense; actions by the Attorney General putting all federal and state law enforcement officials and the U.S. business community on the "highest level of alert"; and the formal announcement of the FBI that the Government had reason to believe that new terrorist attacks might be launched in the United States over the next several days. It was during this period that the President first authorized the program.

Although the intelligence community assessed the threat to be imminent in October 2001, its concerns have persisted to the present day. The United Kingdom aviation plot of August 2006 and the bombing plots in Germany in 2007 are only two of the most recent examples of the continuing threat.

The NSA's activities were reauthorized by the President on a periodic basis through January 2007. Over time, the program was modified to reflect new contingencies. Attorneys from the Office of Legal Counsel of the Department of Justice generated legal opinions throughout the duration of the program.

In a letter to the Congress on January 17, 2007, the Attorney General announced that a judge of the Foreign Intelligence Surveillance Court "had issued orders authorizing the government to target for collection international communications where there is probable cause to believe one of the communicants is a member or agent of al Qaeda or an associated terrorist group. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

THE FISA COURT ORDERS AND FISA MODERNIZATION

On April 12, 2007, the Director of National Intelligence J.M. McConnell submitted to the Congress the Administration's proposal to modernize the Foreign Intelligence Surveillance Act. According to the DNI, the proposal was intended to bring FISA "up to date with the changes in communications technology," preserve "the privacy interests of persons in the United States," and secure assistance from private entities, in part by making certain "they are protected from liability for having assisted the government in its counterterrorism efforts." The Committee held a hearing on the proposal on May 1, 2007, with the DNI, the Director of the National Security Agency, and the Assistant Attorney General for National Security, with additional testimony solicited for the record from a range of experts on national security law and civil liberties.

The Administration's proposal for FISA modernization was comprehensive, and had been coordinated within the Department of Justice and the intelligence community. At the end of May 2007, however, attention was drawn to a ruling of the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information to the Court. In late July, the DNI informed Congress that the decision of the second FISA Court judge had led to degraded capabilities in the face of a heightened terrorist threat environment. The DNI urged the Congress to act prior to the August recess to eliminate the requirement of a court order to collect foreign intelligence about foreign targets located overseas.

THE PROTECT AMERICA ACT

During the final week of July, the House and Senate considered several measures to meet the requirements of the DNI. On August 3, 2007, the Senate adopted S. 1927, the Protect America Act of 2007 (the PAA), and the House passed the bill on August 4, 2007. Signed by the President on August 5, 2007, the PAA authorized the Director of National Intelligence and the Attorney General to acquire foreign intelligence information "concerning" persons outside the United States for one year, if the acquisition involved the assistance of a communication service provider, custodian or other person, and a significant purpose of the collection was the acquisition of foreign intelligence information. The Act was set to sunset after 180 days, on February 1, 2008.

The PAA sparked serious concerns about its reach and scope. The Committee immediately began to review the Act's implementation. The Committee also began a series of consultations to draft a bipartisan proposal to replace the PAA that would authorize the acquisition of foreign intelligence information in light of the advances in technology since 1978 with improved protections for the privacy interests of Americans whose communications might be targeted or incidentally collected. Finally, recognizing the importance of the private sector in assisting law enforcement and intelligence officials in critical criminal justice and national security activities, the Committee reviewed a range of possible responses to pending civil litigation.

TITLE I OF THE FISA AMENDMENTS ACT OF 2007

In the FISA Amendments Act of 2007, the Committee's goal has been to develop a sound legal framework for essential intelligence activities in a manner consistent with the U.S. Constitution. As in the Protect America Act, the Attorney General and the Director of National Intelligence may authorize the targeting of foreign terrorists and other foreign intelligence targets reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence without obtaining individualized court orders from the Foreign Intelligence Surveillance Court, but the bill also significantly increases protections of the civil liberties of U.S. persons located inside and outside the United States.

The FISA Amendments Act of 2007 contains both specific limitations and explicit prohibitions with respect to the collection of U.S. person information. The Protect America Act authorized the acquisition of foreign intelligence information "concerning" persons outside the United States. The vagueness of the word "concerning" created uncertainty as to whether persons inside the United States could be targeted to obtain information "concerning" persons outside the United States. Under this bill, acquisition is permitted only if it "targets" persons who are reasonably believed to be located outside the United States.

In addition, the bill prohibits reverse targeting: conducting surveillance on someone outside the United States for the purpose of targeting a particular known person in the United States. The bill maintains the general requirement that electronic surveillance of a person within the United States for foreign intelligence purposes must be done in accordance with an order from the FISA Court. The bill also requires the Government to obtain an order from the Foreign Intelligence Surveillance Court prior to targeting U.S. persons overseas under the authority of the bill.

The FISA Amendments Act of 2007 increases the role of the FISA Court with respect to targeting under the authority of the Act. Unlike the Protect America Act, the FISA Amendments Act mandates FISA Court review and approval of the minimization procedures governing the protection of the identities and non-public information about U.S. persons. The FISA Amendments Act of 2007 also provides statutory rules for the use of information acquired under the Act, something that was not included in the Protect America Act. The new Title VII created by this bill specifically provides that information from Title VII acquisitions will be governed by the statutory rules that are applicable to electronic surveillance.

The Committee chose to repeal the operative provisions of the Protect America Act in this bill. The Committee set the duration of this Act at six years with the expectation that the Congress would exercise continuing oversight of operations carried out under its authority. The Committee established transition procedures intended to set clear rules for the treatment of orders, authorizations, and directives initiated under the authority of the Foreign Intelligence Surveillance Act both before and after the enactment of the Protect America Act, and under this Act.

The Committee also reaffirmed the 1978 statement in FISA that the Act and provisions of Title 18 are the exclusive means by which electronic surveillance and the interception of domestic communications may be conducted.

Background on Pending Litigation

CIVIL SUITS AGAINST ELECTRONIC COMMUNICATION SERVICE PROVIDERS

After the media reported the existence of a surveillance program in December of 2005, lawsuits were filed against a variety of electronic communication service providers for their alleged participation in the program reported in the media. As of the date of this Committee report, more than forty lawsuits relating to that reported surveillance program had been transferred to a district court in the Northern District of California by the Judicial Panel on Multidistrict Litigation.

The lawsuits allege that electronic communication service providers assisted the federal government in intercepting phone and internet communications of people within the United States, for the purpose of both analyzing the content of particular communications and searching millions of communications for patterns of interest. Some of the lawsuits against the providers seek to enjoin the providers from furnishing records to the intelligence community. Other suits seek damages for alleged statutory and constitutional violations from the alleged provision of records to the intelligence community. Collectively, these suits seek hundreds of billions of dollars in damages from electronic communication service providers.

The Government intervened in a number of these suits to assert the state secrets privilege over particular facts, including whether the companies being sued assisted the Government. The Government also sought to dismiss the suits on state secrets grounds, arguing that the very subject matter of the lawsuits is a state secret. Ultimately, this Government assertion of the state secrets privilege seeks to preclude judicial review of whether, and pursuant to what authorities, any particular provider assisted the Government.

Although the Government has sought to dismiss these suits, the future outcome of this litigation is uncertain. Even if these suits are ultimately dismissed on state secrets or other grounds, litigation is likely to be protracted, with any additional disclosures resulting in renewed applications to the court to allow litigation to proceed.

STATE REGULATORY INVESTIGATIONS

In addition to the civil declaratory judgment and damages suits, a number of state public utilities commissions have opened investigations of electronic communication service providers for their alleged provision of assistance to the intelligence community. These public utilities commissions are seeking to investigate whether the companies violated state privacy rights by providing customer records to agencies of the federal government.

The federal government filed suit seeking to enjoin state officials in five states from further investigation of electronic communication service providers for their alleged disclosure of customer telephone records to the National Security Agency. These cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California in February 2007. In July 2007, the district court found that these state investigations were not preempted by either the Supremacy Clause or the foreign affairs power of the federal government.

The Government may yet prevail in preventing state regulatory investigations of whether particular providers furnished customer records to the intelligence community. But, like the civil suits filed against providers, the outcome of this litigation is uncertain and will likely involve further protracted proceedings.

SUITS AGAINST THE GOVERNMENT

In addition to the lawsuits involving telecommunications providers, a small number of lawsuits were filed directly against the Government challenging the President's surveillance program. These suits allege that the President's program violated the Constitution and numerous statutory provisions, including the exclusivity provisions of the Foreign Intelligence Surveillance Act. These cases are at a variety of different stages of district court and appellate review. Nothing in this bill is intended to affect these suits against the Government or individual Government officials.

TITLE II OF THE FISA AMENDMENTS ACT OF 2007

Title II of this bill reflects the Committee's belief that there is a strong national interest in addressing the extent to which the burden of litigation over the legality of surveillance should fall on private parties. Based on a review of both current immunity provisions and historical information on the President's program, the Committee identified three issues relating to the exposure of electronic communication service providers to liability that needed to be addressed in this bill.

First, the Committee considered the exposure to liability of providers who allegedly participated in the President's surveillance program. Second, the Committee considered the absence, in current law, of a procedural mechanism that would give courts an appropriate role in assessing statutory immunity provisions that would otherwise be subject to the state secrets privilege. Third, the Committee sought to clarify the role of state public utility commissions in regulating electronic communication service providers' relationships with the intelligence community. The Committee addressed these three issues, respectively, in sections 202, 203, and 204 of the bill.

RETROACTIVE IMMUNITY

Sections 201 and 202 of the bill provide focused retroactive immunity for electronic communication service providers that were alleged to have cooperated with the intelligence community in implementing the President's surveillance program. Only civil lawsuits against electronic communication service providers alleged to have assisted the Government are covered under the provision. The Committee does not intend for this section to apply to, or in any way affect, pending or future suits against the Government as to the legality of the President's program.

Section 202 was narrowly drafted to apply only to a specific intelligence program. Section 202 therefore provides immunity for an intelligence activity involving communications that was designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, that was authorized in the period between September 11, 2001 and January 17, 2007, and that was described in written requests to the electronic communication service provider as authorized by the President and determined to be lawful.

The extension of immunity in section 202 reflects the Committee's determination that electronic communication service providers acted on a good faith belief that the President's program, and their assistance, was lawful. The Committee's decision to include liability relief for providers was based in significant part on its examination of the written communications from U.S. Government officials to certain providers. The Committee also considered the testimony of relevant participants in the program.

The details of the President's program are highly classified. As with other intelligence matters, the identities of persons or entities who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence. But it reveals no secrets to say—as the Foreign Intelligence Surveillance Act, this bill, and Title 18 of the U.S. Code all make clear—that electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of the private companies that operate the Nation's telecommunication system.

It would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance. The Committee can say, however, that beginning soon after September 11, 2001, the Executive branch provided written requests or directives to U.S. electronic communication service providers to obtain their assistance with communications intelligence activities that had been authorized by the President.

The Committee has reviewed all of the relevant correspondence. The letters were provided to electronic communication service providers at regular intervals. All of the letters stated that the activities had been authorized by the President. All of the letters also stated that the activities had been determined to be lawful by the Attorney General, except for one letter that covered a period of less than sixty days. That letter, which like all the others stated that the activities had been authorized by the President, stated that the activities had been determined to be lawful by the Counsel to the President.

The historical context of requests or directives for assistance was also relevant to the Committee's determination that electronic communication service providers acted in good faith. The Committee considered both the extraordinary nature of the time period following the terrorist attacks of September 11, 2001, and the fact that the expressed purpose of the program was to "detect and prevent the next terrorist attack" in making its assessment.

On the basis of the representations in the communications to providers, the Committee concluded that the providers, in the unique historical circumstances of the aftermath of September 11, 2001, had a good faith basis for responding to the requests for assistance they received. Section 202 makes no assessment about the legality of the President's program. It simply recognizes that, in the specific historical circumstances here, if the private sector relied on written representations that high-level Government officials had assessed the program to be legal, they acted in good faith and should be entitled to protection from civil suit.

The requirements of section 202 reflect the Committee's determination that cases should only be dismissed when providers acted in good faith. Section 202 applies only to assistance provided by electronics communication service providers pursuant to a "written request or directive from the Attorney General or the head of an element of the intelligence community. . . that the program was authorized by the President and determined to be lawful."

Section 202 also preserves an important role for the courts. Although the bill reflects the Committee's determination that, if the requirements of section 202 are met, the provider acted in good faith, the section allows judicial review of whether the Attorney General has abused the discretion provided by statute in certifying that a provider either furnished no assistance or cooperated with the Government under the terms referenced in the section.

In determining whether to provide retroactive immunity, the Committee weighed the incentives such immunity would provide. As described above, electronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies. Given the scope of the civil damages suits, and the current spotlight associated with providing any assistance to the intelligence community, the Committee was concerned that, without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.

At the same time, the Committee recognized that providers play an essential role in ensuring that the Government complies with statutory requirements before collecting information that may impact the privacy interests of U.S. citizens. Because the Government necessarily seeks access to communications through the private sector, providers have the unparalleled ability to insist on receiving appropriate statutory documentation before agreeing to provide any assistance to the Government.

The Committee sought to maintain the balance between these factors by providing retroactive immunity that is limited in scope. The provision of retroactive immunity was intended to encourage electronic communication service providers who acted in good faith in the particular set of circumstances at issue to cooperate with the Government when provided with lawful requests in the future. Restricting that immunity to discrete past activities avoids disrupting the balance of incentives for electronic communication service providers to require compliance with statutory requirements in the future. Under this bill and existing statutory provisions, providers will only be entitled to protection from suit for their future activities if they ensure that their assistance is conducted in accordance with statutory requirements.

The Committee believes that adherence to precise, existing statutory forms is greatly preferred. This preference is reflected in section 203 of the bill, which establishes procedures by which civil actions against those who assist the Government shall be dismissed upon a certification by the Attorney General that any assistance had been provided pursuant to a court order or a statutorily-prescribed certification or directive. The action the Committee proposes for claims arising out of the President's program should be understood by the Executive branch and providers as a one-time response to an unparalleled national experience in the midst of which representations were made that assistance to the Government was authorized and lawful.

PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES

Section 203 of this bill provides a procedure that can be used in the future to seek dismissal of a suit when a defendant either provided assistance pursuant to a lawful statutory requirement, or did not provide assistance. This section, a new section 802 of FISA, reflects the Committee's recognition that the identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence.

Under the existing statutory scheme, wire or electronic communication providers are authorized to provide information and assistance to persons with authority to conduct electronic surveillance if the providers have been provided with (1) a court order directing the assistance, or (2) a certification in writing signed by the Attorney General or certain other officers that "no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required." See 18 U.S.C. § 2511(2)(a)(ii). Current law therefore envisions that wire and electronic communication service providers will play a lawful role in the Government's conduct of electronic surveillance.

Section 2511(2)(a)(ii) protects these providers from suit as long as their actions are consistent with statutory authorizations. Once electronic communication service providers have a court order or certification, "no cause of action shall lie in any court against any provider of wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter." Id. The Protect America Act and Title I of this bill provide similar protections from suit for providing information or assistance in accordance with statutory directives. All of these immunity provisions are designed to ensure that wire and electronic communication service providers assist the Government with electronic surveillance activities when necessary, and recognize the good faith of those providers who assist the Government in accordance with the statutory scheme.

To the extent that any existing immunity provisions are applicable, however, providers have not been able to benefit from the provisions in the civil cases that are currently pending. Because the Government has claimed the state secrets privilege over the question of whether any particular provider furnished assistance to the Government, an electronic communication service provider who cooperated with the Government pursuant to a valid court order or certification cannot prove it is entitled to immunity under section 2511(2)(a)(ii) without disclosing the information deemed privileged by the Executive branch. Thus, electronic communication providers are prohibited from seeking immunity under section 2511(2)(a)(ii) for any assistance they may have provided to the intelligence community, with the approval of the FISA Court, after January 17, 2007. Providers who did not assist the Government are similarly unable to extract themselves from ongoing litigation, because the assertion of the state secrets privilege makes it impossible for them to demonstrate their lack of involvement.

By addressing the situation in which an entity is prohibited from taking advantage of existing immunity provisions because of Government restrictions on disclosure of the information, Section 203 seeks to ensure that existing immunity provisions have their intended effect. The Committee also intends to reassure providers that as long as their assistance to the Government is conducted in accordance with statutory requirements, they will be protected from civil liability and the burden of further litigation.

The procedure in section 203 allows a court to review a certification as to whether an individual either assisted the Government pursuant to a lawful statutory requirement or did not assist the Government, even when public disclosure of such facts would harm the national security. Because an assertion of state secrets over the same facts would likely prevent all judicial review over whether, and under what authorities, an individual assisted the Government, this provision serves to expand judicial review to an area that may have been previously non-justiciable. In addition, the statute explicitly allows the court to review for abuse of discretion the Attorney General's certification that a person either did not assist the Government or cooperated with the Government pursuant to statutory requirements.

PREEMPTION

Section 204 of the bill preempts state investigations or required disclosure of information about the relationship between individual electronic communication service providers and the intelligence community. The provision reflects the Committee's view that, although states play an important role in regulating electronic communication service providers, they should not be involved in regulating the relationship between electronic communication service providers and the intelligence community.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

OVERALL ORGANIZATION OF BILL

The FISA Amendments Act of 2007 contains three titles.

Title I includes, in section 101, a new Title VII of FISA entitled "Additional Procedures for Targeting Communications of Certain Persons Outside the United States." This new title of FISA (which will sunset in six years) is a successor to the Protect America Act with amendments. Sections 102 through 109 contain a number of amendments to FISA apart from the collection issues addressed in the new Title VII of FISA. These include a provision reaffirming that FISA is the exclusive means for electronic surveillance and important streamlining provisions.

Title II addresses, in accordance with its title, "Protections for Electronic Communication Service Providers." Section 202 establishes a procedure with precise boundaries for liability relief for electronic communication service providers in civil cases involving an intelligence activity authorized by the President between September 11, 2001, and January 17, 2007.

Title II also includes, in sections 203 and 204, a new Title VIII of FISA entitled “Protection of Persons Assisting the Government.” This new title establishes long-term procedures for two matters. One, in section 203, is the manner in which the Government may implement statutory defenses and obtain the dismissal of civil cases against persons, principally electronic communication service providers, who assist elements of the intelligence community in accordance with defined legal documents, namely, orders of the FISA Court or certifications or directives provided for and defined by statute. The other, in section 204, provides for the protection, by way of preemption, of the federal government's ability to conduct intelligence activities without interference by state investigations.

Title III contains important transition procedures for the transition from the Protect America Act to the new Title VII of FISA, as well as authority for the Government to continue to apply to the FISA Court for orders under Title I of FISA in accordance with the law as it stood, in the main, before the Protect America Act. It also contains provisions on the continuation of authorizations, directives, and orders under Title VII that are in effect at the time of the December 21, 2013 sunset, until their expiration within the year following the sunset.

TITLE I. FOREIGN INTELLIGENCE SURVEILLANCE

Section 101. Targeting the communications of persons outside the United States

Section 101(a) of this bill establishes a new Title VII of FISA. Entitled “Additional Procedures for Targeting Communications of Certain Persons Outside the United States,” the new title includes, with important modifications, the authority that had been enacted by the Protect America Act as sections 105A, 105B, and 105C of FISA. Those Protect America Act provisions, which will be repealed by section 302(b)(1) of this bill (or expire on February 1, 2008 in accordance with that Act's 180-day sunset), had been placed within FISA's Title I on electronic surveillance. Moving the amended authority to a title of its own is appropriate because the authority involves not only the acquisition of communications as they are being carried, the province of Title I, but also while they are stored by electronic communication service providers, a form of acquisition akin to physical searches under Title III.

Section 701. Limitation on definition of electronic surveillance

Section 701, as added by Title I of this bill, limits the definition of the term “electronic surveillance,” as that term is defined in Title I of FISA. Two sections added by this bill—section 704 in Title VII on the use of information obtained under Title VII and section 112 in Title I on FISA as the exclusive means for electronic surveillance—negate that limitation for the matters covered by those sections.

The origin of section 701 is section 105A, as added for six months to FISA by the Protect America Act. Described in its heading as a “clarification” applicable to the electronic surveillance of persons outside the United States, section 105A provides that "Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."

Section 701 substitutes the phrase "limitation on definition" for the term "clarification" in order to characterize the provision more accurately.

Section 701 modifies section 105A by explicitly providing that the limitation on the definition of electronic surveillance applies to surveillance that is "targeted in accordance with this title." In other words, the limitation on the Title I definition of electronic surveillance is no broader than the authority under Title VII for electronic surveillance targeted at persons reasonably believed to be outside the United States.

Section 702. Definitions

Section 702 incorporates into Title VII the definition of ten terms that are defined in Title I of FISA and used in Title VII: "agent of a foreign power," "Attorney General," "contents," "electronic surveillance," "foreign intelligence information," "foreign power," "minimization procedures," "United States," "United States person," and "person." It defines the two courts established in Title I that are assigned responsibilities under Title VII: The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review. It also defines "element of the intelligence community" as found in the National Security Act of 1947. Finally, it also defines a term, not previously defined in FISA, that has an important role in setting the parameters of Title VII: "electronic communication service provider."

Section 703. Procedures for acquiring the communications of certain persons outside the United States

Subsection 703(a) sets forth the basic authorization in Title VII, replacing section 105B of the Protect America Act. As had been provided by section 105B, the collection authority in subsection 703(a) is vested in the Attorney General and the Director of National Intelligence, acting jointly, whose authorization shall be for a period of up to one year.

Section 105B and subsection 703(a) differ in an important respect. Section 105B authorized the acquisition of foreign intelligence information "concerning" persons reasonably believed to be outside the United States. To make clear that all collection under Title VII must be targeted at persons who are reasonably believed to be outside the United States, subsection 703(a) eliminates the word "concerning" and instead authorizes "the targeting of persons reasonably believed to be located outside the United States to collect foreign intelligence information."

Subsection 703(b) establishes three related limitations on the authorization in subsection 703(a). One is a specific prohibition on using this authority to target intentionally any person within the United States. The second is that the authority may not be used to conduct "reverse targeting," the intentional targeting of a person reasonably believed to be outside the United States if the purpose of the acquisition is to target for surveillance a person reasonably believed to be in the United States. If that is so, the acquisition must be conducted in accordance with Title I of FISA. The third is an overarching mandate that the authorization in subsection 703(a) shall be used in a manner consistent with the Fourth Amendment to the U.S. Constitution, which provides for "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

Subsection 703(c) addresses United States persons located outside the United States. Subsection 703(c)(1), under the heading of "Acquisition Inside the United States of United States Persons Outside the United States," provides that an acquisition authorized under subsection 703(a) that occurs inside the United States may not target a United States person except in accordance with Title I of FISA.

Subsection 703(c)(2), under the heading of "Acquisition Outside the United States of United States Persons Outside the United States," provides that a U.S. person who is reasonably believed to be outside the United States may not be intentionally targeted if a warrant would be required if the surveillance technique were used in the United States, unless the procedures of the subsection are followed. There are two principal requirements. First, the Attorney General must submit to the FISA Court an application with facts showing there is probable cause that the target is a foreign power or an agent of one, and the court must determine that there is probable cause. Second, the Attorney General must submit to the FISA Court procedures for determining whether a person outside the United States is a U.S. person, the court must approve those procedures, and the procedures must be used.

Subsection 703(d) provides that acquisitions authorized under subsection 703(a) may only be conducted pursuant to a certification of the Attorney General and DNI and in accordance with targeting and minimization procedures that are then subject to judicial review.

Subsection 703(e) provides, in a manner essentially identical to the Protect America Act, for the establishment by the Attorney General, in consultation with the Director of National Intelligence, of targeting procedures that are reasonably designed to ensure that collection is limited to the communications of persons reasonably believed to be outside the United States. As provided in the Protect America Act, the targeting procedures are subject to judicial review.

Subsection 703(f) provides that the Attorney General, in consultation with the Director of National Intelligence shall establish, for acquisitions authorized by subsection 703(a), minimization procedures that are consistent with section 101(h). Section 101(h) is the provision that establishes FISA's minimization requirements for electronic surveillance and physical searches. Subsection 703(f)(2) provides that the minimization procedures, which are essential to the protection of United States citizens and permanent residents, shall be subject to judicial review. This corrects an omission in the Protect America Act which had not provided for judicial review of the adherence of minimization procedures to statutory requirements.

Subsection 703(g) sets forth the elements that must be included in the certification of the Attorney General and the DNI, which include that the targeting and minimization procedures have been approved by the FISA Court or will promptly be submitted to it and that the procedures are consistent with the Fourth Amendment, that a significant purpose of the acquisition is to obtain foreign intelligence information, and that the acquisition involves obtaining that information from or with the assistance of an electronic communication service provider. As with the Protect America Act, the certification is not required to identify the specific facilities, places, premises, or property at which the acquisition under subsection 703(a) will be directed or conducted. The certification shall be submitted to the FISA Court as soon as possible but no later than five days after it is made and be subject to judicial review. The Committee believes that, given that the certification has already been prepared, it should be given promptly to the court.

Subsection 703(h) authorizes the Attorney General and the DNI to direct, in writing with respect to an authorization under subsection 703(a), an electronic communication service provider to provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition. It requires compensation for this assistance and provides that no cause of action shall lie in any court against an electronic communication service provider for its assistance in accordance with a directive. Subsection 703(h) also establishes procedures in the FISA Court for a provider to challenge the legality of a directive or the Government to enforce it. In either case, the question for the court is whether the directive meets the requirements of section 703 and is otherwise lawful.

Subsection 703(i) provides for judicial review of any certification required by subsection 703(d) and the targeting and minimization procedures adopted pursuant to subsections 703(e) and (f). The court shall review certifications to determine whether they contain all the required elements. It shall review targeting procedures to assess whether they are reasonably designed to ensure that the acquisition activity is limited to the targeting of persons reasonably believed to be located outside the United States. The Protect America Act had limited the review of targeting procedures to a "clearly erroneous" standard; subsection 703(i) omits that limitation. With respect to minimization procedures, subsection 703(i) provides that the court shall review them to assess whether they meet the statutory requirement.

If the FISA Court finds that the certification contains all the required elements and that the targeting and minimization procedures are consistent with the requirements of subsections 703(e) and (f) and with the Fourth Amendment, the court shall enter an order approving their continued use for the acquisition authorized by subsection 703(a). If the court does not so find, it shall order the Government, at its election, to correct any deficiencies or cease the acquisition. Acquisitions shall continue during the pendency of any rehearing en banc or appeal to the Foreign Intelligence Surveillance Court of Review.

Subsection 703(j) provides that judicial proceedings under section 703 shall be conducted as expeditiously as possible.

Subsection 703(k) requires that records of proceedings under section 703 shall be maintained under security measures adopted by the Chief Justice in consultation with the Attorney General and the DNI, for the filing of petitions under seal and for review by the FISA Court ex parte and in camera of any Government submission or portions of one that may include classified information, and for retention of directives or orders for not less than 10 years.

Subsection 703(l) provides for oversight of the implementation of Title VII. It has four parts. First, the Attorney General and the DNI shall assess semiannually under subsection 703(l)(1) compliance with the targeting and minimization procedures and submit the assessment to the FISA Court and the congressional intelligence committees. Second, under subsection 703(l)(2), the Inspectors General of the Department of Justice and of any intelligence community element authorized to acquire foreign intelligence under subsection 703(a) are authorized to review compliance of their agency or element with the targeting and minimization procedures. Subsection 703(l)(2)(B) and (C) mandate several numbers that the Inspectors General shall review with respect to United States persons. Their reports shall be submitted to the Attorney General, the DNI, and the intelligence committees. Third, under subsection 703(l)(3), the head of an intelligence community element that conducts a subsection 703(a) acquisition shall review annually whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review is to be submitted to the FISA Court and to the Intelligence Committees. Finally, under subsection 703(l)(4), the Attorney General is to "fully inform" the congressional Intelligence and Judiciary Committees about implementation of the Act at least semiannually.

Section 704. Use of information acquired under Section 703

Section 704 fills a void that has existed under the Protect America Act which had contained no provision governing the use of acquired intelligence. Section 704 provides that information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to Title I for the purposes of section 106, which is the provision of Title I that governs public disclosure or use in criminal proceedings. The one exception is for subsection (j) of section 106, as the notice provision in that subsection, while manageable in individual Title I proceedings, would present a difficult national security question when applied to a Title VII acquisition.

Section 101(b). Table of contents

Section 101(b) of the bill amends the table of contents in the first section of FISA.

Subsection 101(c). Sunset

Section 101(c) of the bill establishes the sunset of the new Title VII of FISA on December 31, 2013.

Section 102. Exclusive means

Section 102 amends Title I of FISA by adding a new Section 112. Under the heading of "Statement of Exclusive Means," the new section states: "Chapters 119 and 121 of Title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) and the interception of domestic wire, oral, or electronic communication may be conducted." It is based on a provision which Congress enacted in 1978 as part of the original FISA that is codified in section 2511(2)(f) of Title 18, United States Code.

Section 112 modifies the Title 18 language in one important respect. To preserve the full application of the exclusive means requirement to "electronic surveillance" as defined from FISA's enactment until the "clarification" of the Protect America Act and the related "limitation" that will be added by this bill, Section 112 provides that the exclusive means requirement applies "regardless of the limitation of section 701."

In agreeing to include this exclusive means provision in their joint mark, the Chairman and Vice Chairman also agreed that the Committee, in this report, should adopt the explanation of the exclusive means requirement that the Conference Committee included in its 1978 report on FISA, H.R. Conf. Rep. No. 95–1720, at 35 (1978). The 1978 conferees noted that the Senate had proposed that FISA be the exclusive means for conducting electronic surveillance, but that the House had countered with an amendment that FISA should be the exclusive "statutory means" of conducting electronic surveillance within the meaning of FISA. The 1978 conference substitute adopted the Senate provision which omitted the word "statutory," as does the present bill.

The 1978 conference report addressed the constitutional implications of the legislation that it was reporting:

> The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter." Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952).

The intent of this Committee is the same. While the exclusive means test in Section 112 does not foreclose the Supreme Court from reaching a different decision, the intent of Section 112 is to place any power of the President to disregard it "at the lowest ebb."

Section 103. Significant interpretations of FISA

Section 6002 of the Intelligence Reform Act and Terrorism Prevention Act of 2004 (Pub. L. 108–458), added a Title VI to FISA that augments the semiannual reporting obligations of the Attorney General to the House and Senate Intelligence and Judiciary Committees. Under it, the Attorney General shall report a summary of significant legal interpretations of FISA in matters before the Foreign Intelligence Surveillance Court or Court of Review. The requirement extends to interpretations presented in applications or pleadings filed with either court by the Department of Justice. In addition to the semiannual summary, the Department of Justice is required to provide copies of court decisions, but not orders, that include significant interpretations of FISA. The importance of the reporting requirement is that, because the two courts conduct their business in secret, Congress needs the reports to know how the law it has enacted is being interpreted.

Section 103 improves the Title VI reporting requirements in two ways. First, as significant legal interpretations may be included in orders as well as opinions, Section 103 requires that orders also be provided to the committees. Second, as the semiannual report often takes many months after the end of the semiannual period to prepare, Section 103 accelerates provision of information about significant legal interpretations by requiring the submission of such decisions, orders, or opinions within 45 days.

OVERVIEW OF SECTIONS 104 THROUGH SECTION 108. FISA STREAMLINING

Sections 104 through 108 amend various sections of FISA for such purposes as reducing a paperwork requirement, modifying time requirements, or providing additional flexibility in terms of the range of Government officials who authorize FISA actions. Collectively, these amendments are described as streamlining amendments. In general, they are intended to increase the efficiency of the FISA process without depriving the Foreign Intelligence Surveillance Court of the information it needs to make findings required under FISA.

Section 104. Applications for court orders under Section 104 of FISA

Section 104 of the bill strikes two of the eleven paragraphs on standard information in an application for a surveillance order under section 104 of FISA, either because the information is provided elsewhere in the application process or is not needed.

In various places, FISA has required the submission of “detailed” information, as in section 104 of FISA, “a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.” The Director of National Intelligence’s legislative proposal asked that “summary” be substituted for “detailed” for this and other application requirements, in order to reduce the length of FISA applications. In general, the Committee’s bill approaches this by eliminating the mandate for “detailed” descriptions, leaving it to the FISA Court and the Government to work out the level of specificity needed by the Court to perform its statutory responsibilities. With respect to one item of information, “a statement of the means by which the surveillance will be effected,” the bill modifies the requirement by allowing for “a summary statement.”

In aid of flexibility, Section 104 increases the number of individuals who may make FISA applications by allowing the President to designate the Deputy Director of the Federal Bureau of Investigation (FBI) as one of those individuals. This should enable the Government to move more expeditiously to obtain certifications when the Director of the FBI is away from Washington or otherwise unavailable.

Subsection (b) of section 104 is eliminated as obsolete in light of current applications. The Director of the Central Intelligence Agency is added to the list of officials who may make a written request to the Attorney General to personally review a FISA application as the head of the CIA had this authority prior to the establishment of the Office of the Director of National Intelligence.

Section 105. Issuance of orders under Section 105 of FISA

Section 105 strikes from Section 105 of FISA several unnecessary or obsolete provisions. Section 105 strikes subsection (c)(1)(F) of Section 105 of FISA which requires minimization procedures applicable to each surveillance device employed because Section 105(c)(2)(A) requires each order approving electronic surveillance to direct the minimization procedures to be followed.

Subsection 6 reorganizes, in more readable form, the emergency surveillance provision of Section 105(f), now redesignated Section 105(e), with a substantive change of extending from 3 to 7 days the time by which the Attorney General must obtain a court order after authorizing an emergency surveillance. The purpose of the change is to help make emergency authority a more practical tool while keeping it within the parameters of FISA.

Subsection 7 adds a new paragraph to Section 105 of FISA to require the FISA Court, on the Government's request, when granting an application for electronic surveillance, to authorize at the same time the installation and use of pen registers and trap and trace devices. This will save the paperwork that had been involved in making two applications.

Section 106. Use of information under Section 106 of FISA

Section 106 amends subsection 106(i) of FISA with regard to the limitations on the use of unintentionally acquired information. Currently, subsection 106(i) provides that unintentionally acquired radio communication between persons located in the United States must be destroyed unless the Attorney General determines that the contents of the communications indicates a threat of death or serious bodily harm to any person. Section 106 amends subsection 106(i) by making it technology neutral on the principle that the same rule for the use of information indicating threats of death or serious harm should apply no matter how the communication is transmitted.

Section 107. Amendments for physical searches

Section 107 makes changes to Title III of FISA: changing applications and orders for physical searches to correspond to changes in Sections 104 and 105 on reduction of some application paperwork; providing the FBI with administrative flexibility in enabling its Deputy Director to be a certifying officer; and extending the time, from 3 days to 7 days, for obtaining a court order after authorization of an emergency search.

Subsection 303(a)(4)(C)—which will be redesignated subsection 303(a)(3)(C)—requires that each application for physical search authority state the applicant's belief that the property is "owned, used, possessed by, or is in transmit to or from" a foreign power or agent of one. In order to provide needed flexibility and to make the provision consistent with electronic surveillance provisions, subsection 107(a)(1)(D) of the bill now being reported allows the FBI to apply for authority to search property that also is "about to be" owned, used, or possessed by a foreign power or agent of one, or in transit to or from one.

Section 108. Amendments for emergency pen registers and trap and trace devices

Section 108 amends Section 403 of FISA to extend from 2 days to 7 days the time for obtaining a court order after an emergency installation of a pen register or trap and trace device. This change harmonizes among FISA's provisions for electronic surveillance, search, and pen register/trap and trace authority the time requirements that follow the Attorney General's decision to take emergency action.

Section 109. Foreign Intelligence Surveillance Court

Section 109 contains three amendments to Section 103 of FISA, which establishes the FISA Court and the Foreign Intelligence Surveillance Court of Review.

Subsection 109(a) amends Section 103 to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement—that the eleven judges be drawn from seven judicial circuits (with the number appearing to be a ceiling rather than a floor)—has proven unnecessarily restrictive or complicated for the designation of the judges to the FISA Court.

Subsection 109(b) amends Section 103 to allow the FISA Court to hold a hearing or rehearing of a matter en banc, that is by all the judges who constitute the FISA Court sitting together. The court may determine to do this on its own initiative, at the request of the Government in any proceeding under FISA, or at the request of a party in the few proceedings in which a private entity or person may be a party, i.e., challenges to document production orders under Title V, or proceedings on the legality or enforcement of directives to electronic communication service providers under Title VII.

Under the section 109(b) amendment, en banc review may be ordered by a majority of the judges who constitute the FISA Court upon a determination that it is necessary to secure or maintain uniformity of the court's decisions or that a particular proceeding involves a question of exceptional importance. It is the intent of the Committee that en banc proceedings should be rare and in the interest of the general objective of fostering expeditious consideration of matters before the FISA Court.

Subsection 109(c) provides authority for the entry of stays, or the entry of orders modifying orders entered by the FISA Court or the Court of Review, pending appeal or review in the Supreme Court. This authority is supplemental to, and does not supersede, the specific provision in section 703(i)(6)(B) that acquisitions under Title VII may continue during the pendency of any rehearing en banc and appeal to the Court of Review.

Section 110. Technical and conforming amendments

This section conforms several provisions of Section 103(e) of FISA in light of the repeal of the Protect America Act and the enactment on the new Title VII.

TITLE II. PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

This title contains four substantive sections. Sections 201 and 202 address liability relief for electronic communication service providers who have been alleged in various civil actions to have assisted the U.S. Government between September 11, 2001, and January 17, 2007, when the Attorney General announced the termination of the Terrorist Surveillance Program. Relating as they do to a particular past matter, these sections are not made a permanent part of FISA. Sections 203 and 204 will enact provisions of a new Title VIII of FISA. They are intended to be permanent provisions for implementing statutory defenses for electronic communication service providers and others who assist the Government in accordance with precise, existing legal requirements, and for providing for federal preemption of state investigations.

Section 201. Definitions

Section 201 establishes definitions for Section 202. Several are of particular importance.

The term "assistance" is defined to mean the provision of, or the provision of access to, information, facilities, or another form of assistance. The word "information" is itself described in a parenthetical to include communication contents, communication records, or other information relating to a customer or communications. "Contents" is defined by reference to its meaning in Title I of FISA. By that reference, it includes any information concerning the identity of the parties to a communication or the existence, substance, purport, or meaning of it.

The term "covered civil action" has two key elements. It is defined as a civil action filed in a federal or state court which (1) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community and (2) seeks monetary or other relief from the electronic communication service provider related to the provision of the assistance. Both elements must be present for the lawsuit to be a covered civil action.

Section 202. Limitations on civil actions for electronic communication service providers

Section 202 provides that, notwithstanding any other provision of law, a covered civil action shall not lie or be maintained in a federal or state court and shall promptly be dismissed if the Attorney General makes a certification to the court that sets forth the elements required by Section 202.

First, the Attorney General must certify that the assistance alleged to have been provided by the electronic communication service provider was in connection with an intelligence activity involving communications that was (1) authorized by the President between September 11, 2001 and January 17, 2007 and (2) designed to detect or prevent a terrorist attack or preparations for one against the United States.

Second, the Attorney General must also certify that the assistance was described in a written request or directive from the Attorney General or the head (or deputy to the head) of an element of the intelligence community to the electronic communication service provider indicating that the activity was (1) authorized by the President and (2) determined to be lawful.

Alternatively, the Attorney General may certify that the electronic communication service provider did not provide the alleged assistance.

The Attorney General's certification is subject to judicial review for abuse of discretion.

If the Attorney General files a declaration that disclosure of a certification would harm national security, the court shall review the declaration in camera and ex parte, which means with only the Government present. A public order following that review shall not disclose whether the certification was based on a written request or directive to the electronic communication service provider for assistance or on the ground that the electronic communication service provider furnished no assistance. The purpose of this requirement is to protect the classified national security information involved in the identification of providers who assist the Government.

Section 203. Procedures for implementing statutory defenses

Section 203 adds two sections of a new Title VIII of FISA.

Section 801 provides for definitions. One, the definition of "assistance," is the same as in Section 201. Another, a definition of "person" (the universe of those protected by Section 802) is necessarily broader than only the definition of electronic communication service provider. This is so because Title VIII applies to all who may be ordered to provide assistance under FISA, such as custodians of records who may be directed to produce records by the FISA Court under Title V of FISA or landlords who may be required to provide access under Title I or III of FISA, not just to electronic communication service providers.

Section 802 establishes procedures for implementing statutory defenses. Notwithstanding any other provision of law, no civil action may lie or be maintained in a federal or state court for assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General makes a certification to the court. The certification must state either that the assistance was not provided or if it was furnished, that it was provided pursuant to a specific existing statutory requirement. The underlying statutory requirements are themselves specifically stated in Section 802: an order of the FISA Court directing assistance, a certification in writing under sections 2511(2)(a)(ii)(B) or 2709(b) of Title 18, or directives to electronic communication service providers under particular sections of FISA or the Protect America Act.

As under Section 202, the Attorney General's certification is subject to judicial review for abuse of discretion. Also, if the Attorney General files a declaration that disclosure of a certification would harm national security, the court shall review it in camera and ex parte. A public order shall not disclose whether the certification was based on an order, certification, or directive, or on the ground that the electronic communication service provider furnished no assistance.

Section 204. Preemption of state investigations

Section 204 adds a Section 803 to the new Title VIII. It addresses investigations that a number of state regulatory commissions have or might begin to investigate cooperation by state regulated carriers with U.S. intelligence agencies. Section 803 preempts these state investigations by prohibiting them and authorizing the United States to bring suit to enforce the prohibition.

Section 205. Technical amendments

Section 205 amends the table of contents of the first section of FISA.

TITLE III. OTHER PROVISIONS

Section 301. Severability

Section 301 provides that if any provision of this Act or its application is held invalid, the validity of the remainder of the Act and its application to other persons and circumstances are unaffected.

Section 302. Effective date; Repeal; Transition procedures

Subsection 302(a) provides that except as provided in the transition procedures, the amendments made by the Act shall take effect immediately.

Subsection 302(b) provides for the repeal of the Protect America Act, except (as provided in subsection 303(c)(1) in the transition procedures) for the immunity established in that Act for the provision of assistance pursuant to a directive under that Act.

Subsection 303(c) establishes five transition procedures in addition to the continuation of immunity for assistance provided under the Protect America Act.

Subsection 303(c)(2)(A) continues in effect orders issued under FISA or under section 6(b) of the Protect America Act in effect on the date of enactment on this new Act, and for their reauthorization under the provisions of FISA in effect on the day before the Protect America Act, except for the exclusive means, reporting, streamlining, and other amendments added by sections 102 through 109 of this new Act (which will be deemed to be part of FISA for such purposes).

Subsection 303(c)(2)(B) provides that any order of the FISA Court issued under Title VII in effect on December 31, 2013, the sunset of Title VII, shall continue in effect until the date of the expiration of such order.

Subsection 303(c)(3)(A) provides that any authorizations or directives of the Attorney General and the Director of National Intelligence in effect on the date of the enactment of this Act issued pursuant to the Protect America Act or any amendment made by that Act shall remain in effect until the date of the expiration of the authorization or directive, and, except as provided by subsection 303(c)(4) of this Act, any acquisition pursuant to such authorization or directive shall be deemed not to be electronic surveillance as that term is defined in 101(f) of FISA, as construed in accordance with section 105A. However, subsection 303(c)(4) establishes that information acquired from an authorization conducted under the Protect America Act shall be deemed to be information acquired from an electronic surveillance pursuant to Title I of FISA for purposes of section 106 of that Act, except for purposes of subsection (j) of such section.

Subsection 303(c)(3)(B) provides similar treatment for any authorizations or directives issued pursuant to this Act in effect on December 31, 2013.

Subsection 303(c)(5) enables the Government to continue to obtain electronic surveillance orders under Title I as it existed the day before the Protect America Act (except as amended by the exclusive means, reporting, streamlining, and other amendments added by sections 102 through 109 of this Act). In other words, notwithstanding the amendments made by the Protect America Act and this new Act to clarify or limit the definition of electronic surveillance and establish a new procedure (now to be in Title VII) for targeting persons reasonably believed to be outside the United States, the Government may continue to use Title I of FISA as if the Protect America Act and the enactment of the new Title VII had never occurred.

Committee Action

VOTE TO REPORT THE COMMITTEE BILL

On October 18, 2007, a quorum for reporting being present, the Committee voted to report the bill favorably, by a vote of 13 ayes and 2 noes. The votes in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—no; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—no; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Warner—aye; Senator Hagel—aye; Senator Chambliss—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Burr—aye.

VOTES ON AMENDMENTS TO COMMITTEE BILL AND THIS REPORT

On October 18, 2007, the Committee rejected an amendment offered by Mr. Nelson to strike Title II, entitled “Protections for Electronic Communications Service Providers,” from the bill, by a vote of 3 ayes and 12 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—no; Senator Wyden—aye; Senator Bayh—no; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—no; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—no; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—no; Senator Burr—no.

On October 18, 2007, the Committee agreed to an amendment offered by Senator Feingold and Senator Wyden to require additional oversight activities by the Inspectors General of the Department of Justice and the intelligence community and the provision of additional information in semi-annual reports to the Congress, by a vote of 8 ayes to 7 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

On October 18, 2007, the Committee agreed to an amendment offered by Senator Wyden, Senator Feingold and Senator Whitehouse to amend the provisions of the bill governing the targeting of U.S.

persons overseas, by a vote of 9 ayes to 6 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

On October 18, 2007, by unanimous consent, the Committee agreed to accept an amendment offered by Senator Feingold concerning the submittal to Congress of certain FISA court orders, as modified by the text of a similar provision of the Intelligence Authorization Act for Fiscal Year 2008 approved by the Senate.

On October 18, 2007, the Committee rejected an amendment offered by Senator Feingold on minimization procedures, the dissemination of foreign intelligence information, and minimization procedures compliance reviews by a vote of 4 ayes to 11 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—no; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—no; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—no; Senator Burr—no.

On October 18, 2007, the Committee rejected an amendment offered by Senator Feingold to change the date applicable to the sunset of the bill from December 31, 2013 to December 31, 2009, by a vote of 3 ayes to 12 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—no; Senator Wyden—aye; Senator Bayh—no; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—no; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—no; Senator Burr—no.

On October 18, 2007, the Committee rejected an amendment offered by Senator Feingold to limit the use of U.S. information obtained through targeting procedures that the FISA Court determines are not reasonably designed to target persons reasonably believed to be overseas, by a vote of 5 ayes to 10 noes. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—no; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—no; Senator Burr—no.

Estimate of Costs

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On October 26, 2007, the Committee transmitted this bill to the Congressional Budget Office and requested it to conduct an estimate of the costs incurred in carrying out its provisions, to the extent not involving classified matters.

Evaluation of Regulatory Impact

In accordance with paragraph 11(b)(2) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to evaluate in this report the regulatory impact of provisions of this bill due to the classified nature of the operations conducted pursuant to this legislation.

Changes in Existing Laws

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

ADDITIONAL VIEWS OF CHAIRMAN ROCKEFELLER

President Bush issued a secret order after September 11th, 2001, authorizing the Intelligence Community to collect without a court order phone and email communications going into and out of the United States where there were reasonable grounds to believe that one party was a member of a terrorist organization.

The expressed purpose of the President's order was to collect intelligence that might help identify terrorists and disrupt their plots before they could be carried out. The President's order, however, also prevented both the judicial and legislative branches of government from carrying out statutorily required oversight of electronic surveillance programs.

The President had a chance to work with Congress in the aftermath of 9/11 to craft a balanced revision to the Foreign Intelligence Surveillance Act (FISA) that would have eliminated the archaic hurdles of targeting foreign agents that had evolved over time while maintaining the essential role the judiciary performs in ensuring the constitutional privacy rights of Americans are not violated in the process.

The President squandered the chance at a critical moment in our Nation's history to unify our efforts in combating the threat of terrorism and instead chose an imperious, go-it-alone approach to governance. In doing so, the Bush Administration sowed the seeds of the program's eventual demise and created a statutory turmoil that Congress is now attempting to resolve.

The President's decision to circumvent the Foreign Intelligence Surveillance Court in carrying out the broad electronic surveillance program and to limit knowledge of the program's existence to only a handful of congressional officials was misguided and undermined the legitimacy and effectiveness of the program.

Ultimately, the Administration was forced to seek and obtain in January 2007 court approval for the collection of electronic communications previously carried out without an order. Efforts by the four congressional oversight committees to fully understand the surveillance program's scope, legal basis, and operational effectiveness have been continually frustrated over many years by an impenetrable cloak of secrecy and a Bush Administration mantra that falsely equates congressional oversight as anathema to national security.

Even now, six years after the warrantless surveillance program was initiated, the Administration continues to withhold from Congress without justification the documents and information it needs to have a full accounting of what happened under the program. The Administration's unwillingness to provide a complete disclosure of these facts is short-sighted and untenable.

Only after the program was disclosed publicly nearly two years ago did the Bush Administration reluctantly agree to brief the entire membership of the Senate and House intelligence committees. At first, the briefings provided were not complete or accurate representations of the program's historical and contemporaneous scope. Glossed over in these delayed briefings as well were the legal concerns within the Administration about the program's operations. As this and other relevant information was being withheld from the Committee, high-ranking officials of the Bush Administration were selectively declassifying and releasing information about the program and falsely assuring the American people that no concerns about the program's legality had been voiced within the Administration.

The Committee will not be dissuaded from completing its review of the President's program. In addition, the reluctance on the part of the Bush Administration to trust and cooperate with Congress unnecessarily alienates those legislators in both parties who wish to work to make our laws stronger and our intelligence capabilities directed at terrorists more robust.

Despite the Bush Administration's distrust of Congress and its inherent resistance to the concept of accountability, the Committee recognized early this year the need to undertake a careful and deliberate review of intelligence collection authorities embodied in the 1978 FISA law.

My goal in undertaking this effort was for the Committee to produce a bipartisan bill that would strengthen our national security, protect the civil liberties and privacy rights of all Americans, and ensure that the unchecked wiretapping policies of the Bush Administration are a thing of the past. The Committee has reported legislation that meets this goal.

The bill, passed on a 13–2 vote, adds the necessary and appropriate court and congressional oversight of surveillance activities that is absent in the flawed Protect America Act hastily passed and signed into law in August. Furthermore, the Committee bill requires that Americans located overseas cannot be targeted for surveillance without court approval, a notable privacy protection not currently in the law.

The bill also includes a narrowly-focused liability provision that protects telecommunications companies from being sued for alleged participation in the surveillance program from 9/11 until it was placed under FISC authorization in January of this year. This immunity provision is not the broad and vague immunity sought by the Administration. The bill does not provide retrospective immunity for government officials for their actions or to companies outside the specified time frame. Nor does the bill extend to criminal proceedings.

The Committee did not endorse the immunity provision lightly. It was the informed judgment of the Committee after months in which we carefully reviewed the facts in the matter. The Committee reached the conclusion that the immunity remedy was appropriate in this case after holding numerous hearings and briefings on the subject and conducting a thorough examination of the letters sent by the U.S. Government to the telecommunications companies.

The Committee determined that telecommunications companies are often asked to be partners in law enforcement and national security efforts, and that their participation was based on what they believed to be lawful directives and representations of the President and the Attorney General.

The assistance of companies is invaluable in carrying out programs that provide for our national security and protect American lives. It is important that this assistance continue and not be extinguished under a deluge of lawsuits.

I believe it is the Bush Administration, not the companies, who must be accountable for the mishandling of the warrantless surveillance program. The internal debate within the Administration over the program was kept from those who participated in the program as well as from the Congress. The Committee, especially now that it finally has access to the President's authorization orders and Department of Justice opinions, will continue its examination of the activities authorized by the President and report its findings. Whatever the conclusions of the Committee may be, the burden of any debate about the conduct of Government officials should not fall on the telecommunications providers who responded to representations made to them after September 11th that the program was legal and that their assistance was required to protect American lives.

JOHN D. ROCKEFELLER IV.

ADDITIONAL VIEWS OF SENATORS BOND, CHAMBLISS, HATCH, AND WARNER

In 1978, Congress passed and the President signed into law the Foreign Intelligence Surveillance Act (FISA). The Act was the result of lengthy debates on the need to strike an appropriate balance between protecting the civil liberties of Americans and using all necessary and appropriate tools to defend the national security of the United States.

FISA served us well for almost thirty years, and, in many ways, it continues to do so. Due to changes in technology, however, FISA began to inhibit vital foreign intelligence collection in ways that Congress never intended. The impact on our intelligence agencies and our troops on the battlefield was profound. Congress acted to correct this problem through the Protect America Act (PAA), which the President signed into law in August 2007. The PAA was enacted as a temporary solution to a serious legal problem that was causing significant intelligence gaps. The PAA is not perfect, but it has done the job it was intended to do. Because the PAA expires in February 2008, it is imperative that Congress pass more permanent changes to FISA.

The FISA Amendments Act is a vitally important piece of legislation that makes long-term improvements and restores much of the original intent of FISA: maintaining the requirement for Foreign Intelligence Surveillance Court (FISC) approval for the electronic surveillance of persons within the United States, while allowing the acquisition of foreign communications without such approval. In addition, the FISA Amendments Act adds new privacy protections for American citizens.

Chairman Rockefeller and I, along with the Director of National Intelligence (DNI), the Department of Justice, and the members of the Senate Intelligence Committee, worked closely together over the past several months to produce this responsible, bipartisan legislation. All of the parties involved had to make significant compromises, but the result is a bill that protects Americans' privacy and civil liberties without unnecessarily hindering the ability of our intelligence agencies to intercept the communications of terrorists and other threats to our national security.

The Senate Intelligence Committee was in a unique position to weigh and assess the many highly classified aspects of our foreign intelligence surveillance operations and to discuss and debate those sensitive issues before we wrote this legislation. The Committee was also entrusted with special access to sensitive national security documents related to this legislation per the Committee's unique jurisdiction over sensitive matters. The resulting Committee bill will work for the Intelligence Community, will work for national security, and will work to protect Americans' privacy interests.

The bill allows the Intelligence Community, through a joint Attorney General and DNI certification, to target the communications of foreign targets outside the U.S. without prior court approval. This provides the speed and agility the Intelligence Community needs and keeps foreign intelligence targets outside of the direct purview of the FISA court, which is what Congress intended when it drafted the FISA bill in 1978. This ensures that foreign collection can continue and that the FISA Court is not bogged down with reviewing numerous foreign collections outside of its purview.

The FISA Amendments Act also ensures the protection of Americans' civil liberties by providing that acquisition may be conducted only in accordance with targeting and minimization procedures adopted by the Attorney General and reviewed by the FISC. Targeting must be consistent with the Fourth Amendment and reverse-targeting of Americans is specifically prohibited. There are also several provisions in the bill that enhance oversight by Congress, the Attorney General, the DNI, and Inspectors General.

One of the most important provisions in this bill is retroactive liability protection for those telecommunication carriers alleged to have assisted the government with the President's Terrorist Surveillance Program (TSP). We believe, without any doubt, that the President properly used his authority under Article II of the Constitution to protect this country in the wake of the 9/11 terrorist attacks. We believe that the TSP was legal, necessary, and most likely prevented another terrorist attack against the homeland.

Those who constantly harp on the misleading assertion that the TSP was illegal conveniently ignore the federal case law that recognizes the President's Article II authority to engage in warrantless surveillance in the context of gathering foreign intelligence. Instead, they assert that the TSP violated FISA. The last time we checked, the Constitution always trumps any statute passed by Congress, including FISA. Even at his lowest ebb, the President still possesses significant authority vis-a-vis Congress in the area of intercepting enemy communications.

I have reviewed the Department of Justice legal opinions and the Presidential authorizations which critics of the TSP had declared would hold the smoking gun that the program was illegal. I have found no smoking gun, and those of us who have seen these documents have found nothing in them that would support the conclusion that the government's actions were illegal. While others may disagree, there should be no doubt that those carriers who are alleged to have participated in the program acted legally and believed that what they were doing was patriotic and in the best interest of the country. These companies deserve to be protected from these costly and frivolous lawsuits. Those who ask why the companies need such protection if they did nothing illegal are missing the fundamental point that the government's invocation of the states secrets privilege precludes these companies from asserting valid defenses and providing the court with any factual evidence confirming or denying their involvement in the program. As a result, these companies cannot defend themselves even if they never participated in the program.

Some have suggested that indemnification of these companies is a better solution. In reality, this is not a suitable fix for the companies, the American taxpayer, or our Intelligence Community. First, lawsuits can be extremely costly to a company in terms of damage to business reputation and stock prices even if that company is ultimately found not liable or if the government pays the legal bills. Second, the American taxpayers have a large enough tax burden and should not be forced to shoulder an additional burden to finance these frivolous lawsuits, filed by parties with no standing or actual damages. We should not use taxpayer funds to line the pockets of trial lawyers seeking to graymail the government into settling these lawsuits to avoid the public disclosure of classified information. Third, the irresponsible and criminal leaks of the TSP and other intelligence programs have been costly to our Intelligence Community. Continuing to litigate these cases against the carriers will risk unnecessary further disclosure of our intelligence sources and methods.

Our enemies are not stupid. They pay attention to our laws and legal proceedings, sometimes better than we do. We have no doubt that they have followed each disclosure or leak of intelligence information with interest. If a person believes that the government has violated his rights, then that individual should pursue legal action against the government. Anyone who wants to pursue legal claims against the government is free to do so under this legislation, but, if we allow these companies to suffer for helping us in the war on terror, could we really blame a company for not wanting to help the next time it is called upon to assist in defending our country?

Unfortunately, the bill contains one very problematic provision, added by amendment, which, if not modified, will make it difficult to get our bill out of the Senate and may make it impossible to get the support of the President who must ultimately sign the bill. This provision prohibits surveillance of U.S. persons who are overseas without a court order. Those in favor of this amendment argue that we should not be conducting surveillance or searches of Americans without a court order. The Fourth Amendment, however, does not always require a warrant. Rather, warrantless surveillances and searches are routinely upheld by courts if they satisfy the reasonableness requirement of the Fourth Amendment. Thus, in the criminal law context, courts have recognized that no warrant is required to conduct a border search, an inventory search, consensual monitoring, certain vehicle searches, etc.

Similarly, under Executive Order 12333, section 2.5, signed by President Reagan in 1981, the Attorney General may authorize surveillances or searches of U.S. persons inside and outside the United States upon a finding of probable cause to believe that that person is a foreign power or an agent of a foreign power. Section 2.5 authority has worked well and without any known abuses. Congress chose in 1978 to leave this authority outside of FISA due to the court's lack of jurisdiction overseas and other complicating intelligence matters. Nevertheless, we support the intent of the amendment: any time a U.S. person is the target of surveillance, the government should get an appropriate judicial ruling. However, since significant technical and legal problems with the provision's language have unintended consequences that would cause the Intelligence Community to lose valuable intelligence on certain U.S. persons who are spying for a foreign power or supporting terrorism, we remain hopeful that we will be able to reach a compromise on this issue when we get to the floor.

As this U.S. person surveillance provision is discussed in the weeks ahead, I want to make sure that all Americans are clear about what individuals would be subject to this provision. The Intelligence Community is not targeting American businessmen traveling overseas on a trip or students studying abroad. It is not targeting ordinary tourists or our soldiers. Instead, they are targeting those few individuals on whom the Intelligence Community seeks to gather foreign intelligence information only after the Attorney General has found probable cause that these U.S. persons are foreign powers or agents of a foreign power. The men and women of our Intelligence Community are honorable people who have taken an oath to protect and defend the Constitution of the United States, and they understand their legal and operational boundaries. It is unfortunate that some are using scare tactics to confuse Americans into thinking that they might be monitored by the U.S. government when traveling overseas. Unless they are spying for a foreign country or supporting terrorism, our government has no foreign intelligence interest in them. Frankly, despite budget increases since 9/11, our Intelligence Community has enough work on its hands tracking terrorists and spies intent on harming us without wasting precious time and resources surveilling innocent Americans.

CHRISTOPHER S. BOND.
SAXBY CHAMBLISS.
ORRIN G. HATCH.
JOHN WARNER.

ADDITIONAL VIEWS OF SAXBY CHAMBLISS

When Congress first considered enacting the Foreign Intelligence Surveillance Act (FISA) it was after some of the most serious intrusions into Americans' lives by the U.S. Intelligence Community were exposed by the Congress. Since 1978, Congress has provided rigorous oversight of our Intelligence Community and enacted valuable legislation, such as FISA, in order to guide our collectors. Congress, and the Intelligence Community, have taken measures to ensure that U.S. citizens are protected from unnecessary government intrusions into their private lives while at the same time balancing the government's need to collect vital intelligence necessary to ward off terrorist attacks or the spies of our enemies. The post 9/11 environment in which Congress must now consider amending FISA is much different from the Cold War era. The threat to the homeland is real and our enemies communicate through more sophisticated means and in a more security conscious manner than in 1978. These evolving threats must be considered by Congress during the debate on FISA modernization. The FISA Amendments Act of 2007 provides much needed updates to FISA, but I am concerned that Congress may not reach this delicate balance without further amending the bill.

The Chairman and Vice Chairman introduced a carefully crafted, bi-partisan piece of legislation. Although it was not a perfect bill, I was willing to forego offering amendments to support the bi-partisan process and provide our Intelligence Community with the minimum requirements it needs in an environment with rapidly changing technology. I believe that the bill which was ultimately adopted by the Committee, and with my support, contains troubling language which should be altered before enactment. I had filed three amendments prior to the Committee's consideration of the FISA Amendments Act of 2007. Although I did not offer any of them, I believe these issues should be addressed by Congress.

My first amendment would change the definition of "electronic surveillance" to make it target-oriented and technology neutral. Rather than carving out an exception to "electronic surveillance" for communications where the target is reasonably believed to be overseas, I believe it would be prudent for the Committee to craft a new definition which focuses on the core question of who is the subject of the surveillance rather than on how or where the communication is intercepted.

When FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time (such as "wire and radio communications"). As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress intended to exclude from FISA's scope. For example, in 1978, most foreign communications went through the air rather than over a wire and most domestic communications were on a wire. Today, most domestic communications, such as cell phone communications, travel through the air and most international communications travel over a wire. The FISA Amendments Act of 2007 seeks to fix this major problem identified by the Director of National Intelligence as a result from this outdated definition, but does so by excluding, or carving out, foreign to foreign communications from the definition of "electronic surveillance" rather than fixing the underlying problem. Although the problem of foreign targeting may be fixed, it is difficult to foresee what additional problems the current technology-based definition may cause in the future. I believe that amending the definition of "electronic surveillance" is the best and most comprehensive solution.

My second amendment would have been a minor technical change deleting the definition of "wire communication." If the definition of "electronic surveillance" is changed, there would no longer be a need to have a definition for "wire communication" since the statute would be technology neutral.

My final amendment sought to strike a provision in the FISA Amendments Act which would require the Foreign Intelligence Surveillance Court (FISC) to review the Attorney General's probable cause determination when the target of surveillance is a known U.S. person overseas and there is probable cause to determine that the individual is a foreign power, agent of a foreign power, or an officer or employee of a foreign power. Instead, Senator Wyden introduced, and the Committee adopted, an amendment requiring that any time a U.S. person is the target of surveillance, regardless of where the collection occurs, the Attorney General must seek FISC approval for that collection.

I am concerned that Senator Wyden's amendment is an attempt by Congress to micromanage the Intelligence Community. Currently, under Executive Order 12333, Section 2.5, the Attorney General may authorize the targeting of a U.S. person overseas upon finding probable cause to believe that the individual is a foreign power or agent of a foreign power. Senator Wyden's amendment seeks to prevent the Intelligence Community from acting quickly and with discretion in a process which has worked well to protect U.S. persons for almost thirty years. The Intelligence Community will now be required to obtain authorization from the FISC prior to conducting surveillance against terrorists or spies overseas who assist foreign governments merely because they are United States persons. It is my belief that the Intelligence Community has demonstrated to Congress how judicious, selective and careful they have been when it comes to protecting the very small number of U.S. citizens this applies to and does not necessarily need the FISC to approve their actions every step along the way.

The Congress considered legislative proposals throughout two Congresses prior to enacting FISA in 1978 and explicitly did not address the issue of U.S. persons overseas because they felt it demanded further consideration. I am concerned that Congress is acting hastily on this subject and moving away from the original intent of FISA. Allowing FISC judges to review the President's constitutional powers to conduct foreign policy and defend the nation is a gross expansion of judicial power from the 1978 FISA law, which was intended to apply solely to domestic surveillance of U.S. persons. Instead of granting oversight of the Executive Branch to judges, Congress should exercise due diligence and reconsider these points after careful examination of the current authorities governing surveillance of U.S. persons overseas. Judges are not elected officials held accountable to the American people like the President and the Congress and it should not be within their jurisdiction to provide after the fact approval or disapproval to the procedures the Executive believes are necessary for our national security.

Finally, I am pleased to see the Committee take responsible action by providing our telecommunications carriers with liability relief. The FISA Amendments Act of 2007 provides that no civil actions may be brought against electronic communication providers if the Attorney General certifies: (1) the assistance alleged was in connection with a communication intelligence activity that was authorized by the President between September 11, 2001 and January 17, 2007, designed to detect or prevent a terrorist attack against the U.S. and described in writing to the provider that it was authorized by the President and lawful; or (2) the communication provider did not provide any of the alleged assistance. It also removes any claims from state courts to the Federal court and preempts any state from conducting an investigation into an electronic communication provider's alleged assistance to the government. The government often needs assistance from the private sector in order to protect our national security and in return they should be able to rely on the government's assurances. America's telecommunication carriers should not have to front heavy legal battles shrouded in secrecy on the government's behalf.

Overall, I support the efforts of the Chairman and Vice Chairman to draft bi-partisan legislation. Whatever form the legislation takes before being presented to the President for his signature, Congress should seek the Director of National Intelligence's comments and advice in order to avoid any unintended consequences from well-intentioned amendments. It is critical that Congress enact FISA legislation, with the input of our core collectors, to ensure that our Intelligence Community has the tools and the legal framework necessary to protect our country from terrorist attacks and to collect vital foreign intelligence information.

SAXBY CHAMBLISS.

ADDITIONAL VIEWS OF SENATORS FEINSTEIN, SNOWE, AND HAGEL

Chairman Rockefeller and Vice Chairman Bond are to be commended for producing a bipartisan bill that the Director of National Intelligence and Department of Justice support. They and their staff have worked together to produce this bill. It is a signal accomplishment, and we commend them.

We believe this legislation is a strong bipartisan bill that will next be reviewed by the Senate Judiciary Committee. We hope that the bill can be further improved, particularly with respect to the issue of FISA's exclusivity, as discussed below.

IMPROVEMENTS IN THIS LEGISLATION

The Committee's bill makes necessary improvements to current law, the Protect America Act that was enacted in August.

Notably, for the first time ever, this legislation would require court review any time the Intelligence Community targets a U.S. citizen for surveillance, regardless of location. Under present law and regulation, the Attorney General can approve surveillance of Americans outside of the country with no judicial review.

This legislation puts the central question before the FISA Court: whether there is probable cause to believe that a U.S. person is an agent of a foreign power. This is a determination that FISA Court judges have made in thousands of instances since 1978, and one to which it is well suited.

In addition, this bill:

- Greatly increases the role of the FISA Court in conducting up-front review and approvals of the targeting and minimization of communications;
- Corrects the concern arising from the Protect America Act that surveillance information could be used in an overly broad manner. Instead, this bill uses FISA's existing limitations on use:
  - Disseminated information must be minimized;
  - Information can only be shared only for appropriate intelligence and law enforcement purposes; and
  - Inadvertently collected intelligence must be destroyed;
- "Streamlines" the FISA application and order process in order to reduce the pending application backlog and the significant amount of time it takes to write and review an application. Specifically, the bill:
  - Allows the government to present a summary, rather than a full description, of how the surveillance will be effected and what intelligence is sought; and
  - Extends the existing FISA "emergency period" from three to seven days during which surveillance may be con-

ducted under the Attorney General's direction prior to a Court order being obtained;

- Provides for strong internal and external oversight by:
  - Requiring the Intelligence Community to conduct an annual review of whether new surveillance authorities are being properly applied;
  - Requiring the Attorney General to provide detailed semi-annual reports to the Senate and House Intelligence and Judiciary committees concerning collections authorized in the bill—including instances of non-compliance; and
  - Authorizing the Inspectors General of the Department of Justice and elements of the Intelligence Community to conduct independent reviews of agency compliance with the court-approved acquisition and minimization procedures.
- Clearly prohibits warrantless surveillance against persons inside the United States.

Legislation amending the Foreign Intelligence Surveillance Act of 1978, and the Protect America Act that was passed in August of this year, will only succeed if it is bipartisan. In this area, it is our belief that any partisan bill will not pass.

That outcome is likely to result in one of two unacceptable options:

- A rushed process to extend the Protect America Act, which contains fewer statutory protections of privacy rights than the Committee's bill, or
- A lapse in legislation, which will prevent the Intelligence Community from conducting much-needed surveillance on non-United States citizens outside of the country.

Clearly, passing meaningful reforms should be a top priority of the U.S. Congress.

EXCLUSIVITY OF FISA

The legislation includes language on the exclusivity of FISA that requires further examination. Section 102 of the Intelligence Committee bill states that the Foreign Intelligence Surveillance Act and relevant portions of Title 18 of the U.S. Code are the "exclusive means" by which "electronic surveillance" may be conducted.

The definition of the term "electronic surveillance," however, was written in 1978 and has been the subject of exemptions and limitations since then.

It is essential that the Committee determine whether there are any intelligence techniques that fall within this legislation's scope for which the Executive Branch may not follow the bill's procedures. This is a necessarily classified topic, but we intend to conduct careful review of these techniques before this legislation is enacted.

It is our view that the Foreign Intelligence Surveillance Act, as amended, should be the only legal way of acquiring the communications of people inside the United States, and U.S. persons outside the United States in certain circumstances, for foreign intelligence purposes.

There is a history to this provision that makes a strong congressional re-affirmation even more important.

The legislative history from when FISA was originally enacted in 1978 is quite clear. It states:

> [d]espite any inherent power of the President to authorize warrantless electronic surveillance in the absence of legislation, by this bill and chapter 119 of title 18, Congress will have legislated with regard to electronic surveillance in the United States, that *legislation with its procedures and safeguards prohibit the President, notwithstanding any inherent powers, from violating the terms of that legislation*. (emphasis added)

The legislative history continued by describing the Supreme Court's decision in the Keith case, in which the Court ruled that at that time, Congress hadn't ruled in this field and "simply left the presidential powers where it found them." But at this point, the legislative history turns. It said:

> The Foreign Intelligence Surveillance Act, however, does not simply leave Presidential powers where it finds them. To the contrary, this bill would *substitute a clear legislative authorization pursuant to statutory, not constitutional, standards.* (emphasis added)

This was the statement accompanying H.R. 7138 as it passed the 95th Congress. It is clear that Congress enacted the 1978 legislation with the specific intent that it would be the only authority under which foreign intelligence could be obtained from electronic surveillance.

It is also clear that President Carter was aware of this intent when he signed the bill into law. President Carter's signing statement noted that:

> The bill requires, for the first time, a prior judicial warrant for all electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign intelligence by electronic surveillance in the United States. It will remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism . . . . (emphasis in original)

This intent, and FISA practice for more than 20 years, was cast in doubt after September 11, 2001. At that time, the Executive Branch concluded that it was not bound by FISA's procedures, and proceeded with the Terrorist Surveillance Program (TSP) without requesting amendments to FISA.

As explained in the Department of Justice's 2006 White Paper on the legality of the TSP, the Administration cited the Authorization for the Use of Military Force (AUMF) against al Qaeda and its supporters as an alternative authority. The Department pointed to language in FISA that it was exclusive except as authorized by other statute.

Congress intended for the “other statute” to be the laws governing criminal wiretaps, not a broad and undefined exception.

We do not believe that the AUMF provided this authorization. We have seen no evidence that Congress intended the AUMF to authorize a widespread effort to collect the content of Americans’ phone and email communications, nor does the AUMF refer to the subject.

Furthermore, FISA already contained a provision that clearly governed surveillance actions in a wartime situation—a 15–day authorization for warrantless surveillance following a declaration of war. So this was not an uncontemplated question following September 11 and the passage of the AUMF.

More troubling, however, is the Administration’s claim that the Constitution would not allow FISA to limit the President’s ability to conduct surveillance and other activities covered by that legislation in any way he sees fit. The Department of Justice argues that Congress has not, and cannot, so limit the Executive’s power.

For these reasons, we continue to believe that Congress must write strong language to ensure that FISA is the exclusive means that the Intelligence Community may intercept, analyze, and disseminate the phone and electronic communications of any American for intelligence purposes.

We will work to strengthen the exclusivity language as the bill progresses.

Achieving the balance between necessary intelligence collection and the protection of Americans’ privacy rights is perhaps nowhere as difficult as in the areas surrounding FISA. It is not a field in which partisan politics should play a part. Nor is it one where the Congress and the President should be in conflict.

We thank again Chairman Rockefeller and Vice Chairman Bond for their work on this legislation. It is a big step forward.

DIANNE FEINSTEIN.
OLYMPIA J. SNOWE.
CHUCK HAGEL.

ADDITIONAL VIEWS OF SENATOR NELSON

I strongly support the efforts of Chairman Rockefeller and Vice-Chairman Bond to craft a compromise that a bipartisan majority of the SSCI supported. This bill strikes the right balance, protecting Americans' privacy while giving the government the tools that it needs to stop terrorists.

During the committee's mark-up of the bill, I offered an amendment that would have struck Title II from the bill. Title II provides immunity to any telecommunications company that may have provided assistance to the government under the President's warrantless surveillance program between September 11, 2001 and January 17, 2007.

I am sympathetic to the notion that companies may have acted in good faith to provide the government with assistance during a national security crisis, but I believe it's premature to grant them immunity. The committee received critical documents only 48 hours before the vote. I believe we need more time to gain a full understanding of the President's warrantless surveillance program before deciding whether the companies should receive retroactive immunity.

I voted to support the bill because legislation that provides protections for Americans while enabling the government to get the information it needs to stop terrorists is necessary and immediate.

BILL NELSON.

ADDITIONAL VIEWS OF SENATOR WHITEHOUSE

With this legislation, the Senate takes an important step forward to repair damage the Bush Administration has done to the privacy and security of innocent American citizens. The President's warrantless wiretapping program provoked dismay and outrage not only in my home state of Rhode Island, but throughout the nation. This outrage has continued largely unabated as the President has delayed and circumscribed efforts by the American people's representatives to determine what took place under the secret program. This legislation moves the Government toward a solution that gives the law enforcement and intelligence communities the resources they need to keep us secure, but also upholds the critical balance of law and principle upon which that security depends.

I know such a solution exists. I saw it in action during my years as a federal and state prosecutor. But rather than seek that common-sense solution, this President chose to trample on the rights of the very people he was sworn to protect, and left millions of Americans wondering whether they can trust their government.

In August, I voted against the Protect America Act, a flawed law rushed through Congress under intense political pressure from the Administration, because the law amended the Foreign Intelligence Surveillance Act (FISA) in a way that did not adequately protect the rights of American citizens who are caught up in warrantless government surveillance. I voted for the new bill in the Senate Select Committee on Intelligence because it takes a significant step away from the flawed August law and toward the protection of civil liberties. It is a significant first step in the four-step process that I hope will lead us to a bill that both protects Americans' privacy rights and strengthens our ability to conduct essential foreign intelligence surveillance.

Everyone agrees that United States intelligence agencies should be able to wiretap foreign targets overseas without judicial authorization. The problem we are obliged to address, but failed to address adequately in the August law, emerges when surveillance overseas implicates: (1) U.S. citizens who happen to be abroad; or (2) U.S. citizens in America whose communications are intercepted incidentally, for instance when they communicate with a surveilled target.

There are simple touchstones for protecting Americans' rights in this context: the principles that guide domestic law enforcement surveillance. When I served as a United States Attorney and as Rhode Island Attorney General, I sought, obtained, and oversaw wiretaps in gang, narcotics, and public corruption investigations. Two fundamental principles prevailed. First, the government cannot target Americans for surveillance without the approval of a judge. Second, surveilling agents are required by the court to "minimize" the surveillance if it is not relevant to the investigation.

This helps protect innocent citizens who are not the target, but who talk to the target.

I have worked closely with the Chairman and other members of the Committee to strengthen protections for U.S. citizens in the new bill, including by proposing and supporting a number of amendments. The new bill ensures the involvement and oversight of the Foreign Intelligence Surveillance Court when U.S. citizens abroad are targeted. I cosponsored and strongly supported an amendment, proposed by Senator Wyden, and approved by the Committee, that requires the Government to obtain a traditional warrant from the Foreign Intelligence Surveillance Court (FISC) if the Government wants to collect, from a source within the United States, against an American overseas. The amendment also requires that, in order to collect surveillance overseas on a U.S. citizen traveling or living overseas, the Government obtain a determination from the FISC that the targeted U.S. citizen is a foreign power or the agent of a foreign power. Furthermore, the FISC must issue an ex parte order approving this surveillance. These changes are critical to ensuring that the new warrantless surveillance authority enacted under the Protect America Act does not allow the Government to intrude inappropriately upon the privacy of U.S. citizens. Nonetheless, the Administration has already signaled that this amendment may create certain challenges that need to be resolved. If the Administration intends to propose an alternative, it must preserve the Court's role in determining whether there is probable cause to believe the U.S. citizen is a foreign power or an agent of a foreign power. U.S. citizens do not, and should not be expected to, leave their privacy rights behind every time they leave the United States.

In protecting the privacy of Americans while conducting surveillance, the critical element is judicial oversight. In the August law, the FISC was authorized only to review the Government's determination that its surveillance targets persons "reasonably believed to be outside the United States"—and to intervene only if the Government's determination is "clearly erroneous." In contrast, under this bill, the FISC will need to approve both the "targeting" determination and the "minimization" procedures that are designed to protect U.S. citizens in America whose communications are intercepted incidentally. This bill also rejects the unduly permissive standard of review that the August law had imposed.

While these changes are positive and significant, there remains important work to be done to improve the bill. The FISC should not be required to approve the minimization procedures for warrantless surveillance of Americans and then forced to ignore their implementation. I have drafted and introduced an amendment that would clarify that the FISC has the same powers to review the Government's compliance with minimization procedures for warrantless surveillance as it does with the minimization procedures used pursuant to traditional FISA warrants. This change is not yet a part of the bill, but I will continue to press for the Court's clear authority to check on the implementation of these minimization procedures. U.S. citizens whose communications are incidentally intercepted should enjoy a two-stage protection: the minimization procedures themselves, and the salutary prospect of judicial review of compliance. Engaging more than one branch of government is a traditional protection in our American system of government. Here, those checks and balances can be exercised in a way that is neither burdensome nor disruptive to intelligence-gathering operations. As the bill continues to move through the legislative process, I will seek to strengthen the protections for U.S. citizens.

Finally, Congress is seeking to revise FISA in light of a program that was conducted outside its framework. As it acts, Congress must leave no shadow of a doubt that the Foreign Intelligence Surveillance Act, as amended, is the exclusive means for authorizing foreign intelligence surveillance. I will stand as a strong supporter of Senator Feinstein's efforts to prevent this Administration or future ones from acting outside this law.

SHELDON WHITEHOUSE.

MINORITY VIEWS OF SENATORS FEINGOLD AND WYDEN

As strong opponents of the Protect America Act, we have been very concerned about the vast new authorities granted under that legislation, as well as the possibility that its vague language will be interpreted by the executive branch to permit even broader surveillance than has already been acknowledged publicly. We support the underlying purpose of FISA reform: to permit the government to conduct surveillance of foreign targets, particularly terrorist suspects, as they communicate with other persons overseas, without having to obtain a FISA court order. We believe that this purpose can be achieved while protecting the rights and privacy of law-abiding Americans conducting international communications. We believe that the bill that passed the Senate Intelligence Committee unfortunately falls short of that goal in some respects, and we are also concerned that it also provides sweeping retroactive immunity to those alleged to have cooperated with the President's warrantless wiretapping program. We were therefore disappointed with the bill and voted against it. We look forward to the opportunity to debate further modifications to this bill as it passes through the Judiciary Committee and onto the Senate floor.

We were pleased, however, that three amendments we offered passed. One amendment, which we offered along with Senator Whitehouse, ensures that whenever the government wants to target an American overseas, the FISA Court—and not just the Attorney General—must determine that there is probable cause that the American is an agent of a foreign power. Americans' rights should not diminish when they cross the border, nor should the extent of those rights be subject to the whim of the executive branch without the checks and balances provided by the court.

Another amendment adopted by the Committee ensures that the Department of Justice Inspector General and other Inspectors General have the information they need to review fully how the new authorities are implemented. It also requires that the Administration provide Congress with additional information—including access to reports and documentation—so that Congress can assess how the legislation is being used. For purposes of oversight and possible reauthorization at the end of a sunset period, this information is critical. In addition, an amendment offered by Senator Feingold and accepted by the Committee ensures that any FISA Court legal opinions related to the new authorities will be provided, in a timely manner, to Congress.

Despite these improvements, the bill fails to protect the privacy rights of Americans in critical areas addressed in other amendments we either offered or filed. One such amendment, filed by Senator Feingold, would have permitted ongoing surveillance of persons overseas, but directed that if the government knows that certain communications involved persons in the United States, those communications with the U.S. would have to be sequestered and would be accessible to government agents only with the approval of the FISA Court or in emergencies. This amendment would grant the flexibility the administration has said it needs while providing protection to law-abiding Americans making international calls. It also recognizes that, given the broad new authorities provided by the PAA and this new legislation, non-statutory, classified minimization procedures do not provide the independent review needed to protect the privacy of Americans. We were disappointed that the Committee rejected an amendment offered by Senator Feingold that would have provided for stronger, more effective minimization procedures. The amendment would have limited the types of U.S. person information that could be disseminated to information necessary to protect against terrorism and other threats to national security, ensured that the FISA Court has sufficient information to assess compliance with minimization procedures, and given the FISA Court the authority to review and enforce that compliance. This amendment was a limited alternative to a FISA Court order requirement, and its defeat leaves in place what we believe are inadequate mechanisms for protecting the privacy of Americans' communications.

We are also concerned about the lack of incentives for the government to target only those persons who are overseas in the first place. The bill improves upon the PAA by removing a "clearly erroneous" standard for FISA court review of the procedures the government uses to ensure that surveillance targets are reasonably likely to be overseas. But there are no consequences to the government if the court determines that the government's procedures are not reasonably designed to target persons reasonably believed to be overseas. The government cannot use those procedures going forward, but it can retain and share everything it learned through the use of the unlawful procedures up until the point when the Court rejected them. We therefore supported an amendment offered by Senator Feingold that would have limited the use of U.S. person information obtained through targeting procedures later rejected by the court. The defeat of that amendment means that, even when the court finds that the government's procedures are targeting Americans in the United States without a warrant, the government can continue to use the information obtained through that surveillance however it sees fit. This loophole offers an invitation to warrantless wiretapping.

Senator Wyden filed an amendment that would have limited the scope of the authorities to foreign intelligence information related to national security threats. The Administration's stated purpose for the PAA, and the purported emergency that drove the precipitous passage of that legislation, was the terrorist threat to the United States. We strongly support providing the government the authorities it needs to detect terrorists and other national security threats and believe that this can be done while protecting the rights and privacy interests of Americans. We do not believe, however, that broad new authorities related to any communications involving any foreign intelligence (a term that is very broadly defined) are justified, particularly in the absence of the kinds of oversight and checks and balances needed to defend the rights of Americans and protect against abuses.

Another amendment we filed would have required that a court order be obtained when a "significant purpose" of the wiretapping is to obtain information on an American talking to a foreign target. The Director of National Intelligence has stated publicly that "reverse targeting" is a violation of the 4th Amendment to the United States Constitution and subject to criminal prosecution. This amendment would have provided some protection for this constitutional principle and would have prevented the government from using its foreign targeting authorities to obtain information on Americans. We are concerned that the language that remains in the bill—prohibiting only surveillance when the purpose of the surveillance is to obtain information on an American—may not protect against the government targeting a person overseas as a fig leaf for surveillance of the American with whom the overseas person is communicating.

We strongly supported Senator Nelson's amendment to strip from the bill a provision providing blanket immunity to private entities alleged to have cooperated with the Administration's warrantless wiretapping program. The arrangements made by the Administration the week of the mark-up to provide limited access to certain documents related to the program were unfortunately inadequate. More importantly, nothing in the documents, or anything else that we have seen in the course of our review of the program, has convinced us that a sweeping grant of immunity for private entities should have been included in this legislation.

Finally, we were extremely disappointed that a Feingold amendment to shorten the six-year sunset to two years did not pass. The vast new authorities provided under the PAA, the ongoing confusion about how legislation in this area is and will be interpreted, and ongoing changes in telecommunications technology require that Congress conduct a near-term assessment of how this legislation is being interpreted and implemented and whether changes to the new authorities are needed. In our view, Congress should not wait until 2013 to conduct this thorough review.

RUSSELL D. FEINGOLD.
RON WYDEN.

○

Exhibit 2

H.R. 6304, FISA AMENDMENTS ACT OF 2008

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

Senator John D. Rockefeller IV, Chairman of the Select Committee on Intelligence

The consideration of legislation to amend the Foreign Intelligence Surveillance Act of 1978 ("FISA") in the 110th Congress began with submission by the Director of National Intelligence ("DNI") on April 12, 2007 of a proposed Foreign Intelligence Surveillance Modernization Act of 2007, as Title IV of the Administration's proposed Intelligence Authorization Act for Fiscal Year 2008. The DNI's proposal was the subject of an open hearing on May 1, 2007 and subsequent closed hearings by the Senate Select Committee on Intelligence, but was not formally introduced. It is available on the Committee's website: http://intelligence.senate.gov/070501/bill.pdf. In the Senate, the original legislative vehicle for the consideration of FISA amendments in the 110th Congress was S. 2248. It was reported by the Select Committee on Intelligence on October 26, 2007 (S. Rep. No. 110-209 (2007)), and then sequentially reported by the Committee on the Judiciary on November 16, 2007 (S. Rep. No. 110-258 (2008)). In the House, the original legislative vehicle was H.R. 3773. It was reported by the Committee on the Judiciary and the Permanent Select Committee on Intelligence on October 12, 2007 (H. Rep. No. 110-373 (Parts 1 and 2)(2007)). H.R. 3773 passed the House on November 15, 2007. S. 2248 passed the Senate on February 12, 2008, and was sent to the House as an amendment to H.R. 3773. On March 14, 2008, the House returned H.R. 3773 to the Senate with an amendment.

No formal conference was convened to resolve the differences between the two Houses on H.R. 3773. Instead, following an agreement reached without a formal conference, the House passed a new bill, H.R. 6304, which contains a complete compromise of the differences on H.R. 3773.

H.R. 6304 is a direct descendant of H.R. 3773, as well as of the original Senate bill, S. 2248, and the legislative history of those measures constitutes the legislative history of H.R. 6304. The section-by-section analysis and explanation set forth below is based on the analysis and explanation in the report of the Select Committee on Intelligence on S. 2248, at S. Rep. No. 110-209, pp. 12-25, as expanded and edited to reflect the floor amendments to S. 2248 and the negotiations that produced H.R. 6304.

OVERALL ORGANIZATION OF ACT

The FISA Amendments Act of 2008 ("FISA Amendments Act") contains four titles.

Title I includes, in section 101, a new Title VII of FISA entitled " Additional Procedures Regarding Certain Persons Outside the United States." This new title of FISA (which will sunset in four and a half years) is a successor to the Protect America Act of 2007, Pub. L. 110-55 (August 5, 2007) ("Protect America Act"), with amendments. Sections 102 through 110 of the Act contain a number of amendments to FISA apart from the collection issues addressed in the new Title VII of FISA. These include a provision reaffirming and strengthening the requirement that FISA is the exclusive means for electronic surveillance, important streamlining provisions, and a change in the definitions section of FISA (in section 110 of the bill) to facilitate foreign intelligence collection against proliferators of weapons of mass destruction.

Title II establishes a new Title VIII of FISA which is entitled "Protection of Persons Assisting the Government." This new title establishes a long-term procedure, in new FISA section 802, for the Government to implement statutory defenses and obtain the dismissal of civil cases against persons, principally electronic communication service providers, who assist elements of the intelligence community in accordance with defined legal documents, namely, orders of the FISA Court or certifications or directives provided for and defined by statute. Section 802 also incorporates a procedure with precise boundaries for liability relief for electronic communication service providers who are defendants in civil cases involving an intelligence activity authorized by the President between September 11, 2001, and January 17, 2007. In addition, Title II provides for the protection, by way of preemption, of the federal government's ability to conduct intelligence activities without interference by state investigations.

Title III directs the Inspectors General of the Department of Justice, the Department of Defense, the Office of National Intelligence, the National Security Agency, and any other element of the intelligence community that participated in the President's Surveillance Program authorized by the President between September 11, 2001, and January 17, 2007, to conduct a comprehensive review of the program. The Inspectors General are required to submit a report to the appropriate committees of Congress, within one year, that addresses, among other things, all of the facts necessary to describe the establishment, implementation, product, and use of the product of the President's Surveillance Program, including the participation of individuals and entities in the private sector related to the program.

Title IV contains important procedures for the transition from the Protect America Act to the new Title VII of FISA. Section 404(a)(7) directs the Attorney General and the DNI, if they seek to replace an authorization under the Protect America Act, to ***S6130** submit the certification and procedures required in accordance with the new section 702 to the FISA Court at least 30 days before the expiration of such authorizations, to the extent practicable. Title IV explicitly provides for the continued effect of orders, authorizations, and directives issued under the Protect America Act, and of the provisions pertaining to protection from liability, FISA court jurisdiction, the use of information acquired and Executive Branch reporting requirements, past the statutory sunset of that act. Title IV also contains provisions on the continuation of authorizations, directives, and orders under Title VII that are in effect at the time of the December 31, 2012 sunset, until their expiration within the year following the sunset.

TITLE I. FOREIGN INTELLIGENCE SURVEILLANCE

Section 101. Targeting the Communications of Persons Outside the United States

Section 101(a) of the FISA Amendments Act establishes a new Title VII of FISA. Entitled "Additional Procedures Regarding Certain Persons Outside the United States," the new title includes, with important modifications, an authority similar to that granted by the Protect America Act as temporary sections 105A, 105B, and 105C of FISA. Those Protect America Act provisions had been placed within FISA's Title I on electronic surveillance. Moving the amended authority to a title of its own is appropriate because the authority involves not only the acquisition of communications as they are being carried but also while they are stored by electronic communication service providers.

Section 701. Definitions

Section 701 incorporates into Title VII the definition of nine terms that are defined in Title I of FISA and used in Title VII: "agent of a foreign power," "Attorney General," "contents," "electronic surveillance," "foreign intelligence information," "foreign power," "person," "United States," and " United States person." It defines the congressional intelligence committees for the purposes of Title VII. Section 701 defines the two courts established in Title I that are assigned responsibilities under Title VII: the Foreign Intelligence Surveillance Court ("FISA Court") and the Foreign Intelligence Surveillance Court of Review. Section 701 also defines "intelligence community" as found in the National Security Act of 1947. Finally, section 701 defines a term, not previously defined in FISA, which has an important role in setting the parameters of Title VII: "electronic communication service provider." This definition is connected to the objective that the acquisition of foreign intelligence pursuant to this title is meant to encompass the acquisition of stored electronic communications and related data.

Section 702. Procedures for Targeting Certain Persons Outside the United States Other than United States Persons

Section 702(a) sets forth the basic authorization in Title VII, replacing section 105B of FISA, as added by the Protect America Act. Unlike the Protect America Act, the collection authority in section 702(a) is to be conducted pursuant to the issuance of an order of the FISA Court, or pursuant to a determination of the Attorney General and the DNI, acting jointly, that exigent circumstances exist, as defined in section 702(c)(2), subject to subsequent and expeditious action by the FISA Court. Authorizations must contain an effective date, and may be valid for a period of up to one year from that date.

Subsequent provisions of the Act implement the prior order and effective date provisions of section 702(a): in addition to section 702(c)(2) which defines exigent circumstances, section 702(i)(1)(B) provides that the court shall complete its review of certifications and procedures within 30 days (unless extended under section 702(j)(2)); section 702(i)(5)(A) provides for the submission of certifications and procedures to the FISA Court at least 30 days before the expiration of authorizations that are being replaced, to the extent practicable; and section 702(i)(5)(B) provides for the continued effectiveness of expiring certifications and procedures until the court issues an order concerning their replacements.

Section 105B and section 702(a) differ in other important respects. Section 105B authorized the acquisition of foreign intelligence information " concerning" persons reasonably believed to be outside the United States. To make clear that all collection under Title VII must be targeted at persons who are reasonably believed to be outside the United States, section 702(a) eliminates the word "concerning" and instead authorizes "the targeting of persons reasonably believed to be located outside the United States to collect foreign intelligence information."

Section 702(b) establishes five related limitations on the authorization in section 702(a). Overall, the limitations ensure that the new authority is not used for surveillance directed at persons within the United States or at United States persons. The first is a specific prohibition on using the new authority to target intentionally any person within the United States. The second provides that the authority may not be used to conduct "reverse targeting," the intentional targeting of a person reasonably believed to be outside the United States if the purpose of the acquisition is to target a person reasonably believed to be in the United States. If the purpose of the acquisition is to target a person reasonably believed to be in the United States, the acquisition must be conducted in accordance with other titles of FISA. The third bars the intentional targeting of a United States person reasonably believed to be outside the United States. In order to target such United States person, acquisition must be conducted under three subsequent sections of Title VII, which require individual FISA court orders for United States persons: sections 703, 704, and 705. The fourth limitation goes beyond targeting (the object of the first three limitations) and prohibits the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. The fifth is an overarching mandate that an acquisition authorized in section 702(a) shall be conducted in a manner consistent with the Fourth Amendment to the U.S. Constitution, which provides for "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

Section 702(c) governs the conduct of acquisitions. Pursuant to section 702(c)(1), acquisitions authorized under section 702(a) may be conducted only in accordance with targeting and minimization procedures approved at least annually by the FISA Court and a certification of the Attorney General and the DNI, upon its submission in accordance with section 702(g). Section 702(c)(2) describes the "exigent circumstances" in which the Attorney General and Director of National Intelligence may authorize targeting for a limited time without a prior court order for purposes of subsection (a). Section 702(c)(2) provides that the Attorney General and the DNI may make a determination that exigent circumstances exist because, without immediate implementation of an authorization under section 702(a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to section 702(i)(3) prior to the implementation of such authorization. Section 702(c)(3) provides that the Attorney General and the DNI may make such a determination before the submission of a certification or by amending a certification at any time during which judicial review of such certification is pending before the FISA Court.

Section 702(c)(4) addresses the concern, reflected in section 105A of FISA as added by the Protect America Act, that the definition of electronic surveillance in Title I might prevent use of the new procedures. To address this concern, section 105A redefined the term "electronic surveillance" to exclude "surveillance directed at a person reasonably believed to be located outside of the United States." This redefinition, however, broadly exempted activities from the limitations of FISA's individual order requirements. In contrast, section 702(c)(4) does not change the definition of electronic surveillance, but clarifies the intent of Congress to allow the targeting of foreign targets outside the United States in accordance with section 702 without an application for a court order under Title I of FISA. The addition of this construction paragraph, as well as the language in section 702(a) that an authorization may occur "notwithstanding any other law," makes clear that nothing in Title I of FISA shall be construed to require a court order under that title for an acquisition that is targeted in accordance with section 702 at a foreign person outside the United States.

Section 702(d) provides, in a manner essentially identical to the Protect America Act, for the adoption by the Attorney General, in consultation with the DNI, of targeting procedures that are reasonably designed to ensure that collection is limited to targeting persons reasonably believed to be outside the United States. As provided in the Protect America Act, the targeting procedures are subject to judicial review and approval. In addition to the requirements of the Protect America Act, however, section 702(d) provides that the targeting procedures also must be reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. Section 702(d)(2) subjects these targeting procedures to judicial review and approval.

Section 702(e) provides that the Attorney General, in consultation with the DNI, shall adopt, for acquisitions authorized by section 702(a), minimization procedures that are consistent with section 101(h) or 301(4) of FISA, which establish FISA's minimization requirements for electronic surveillance and physical searches. Section 702(e)(2) provides that the minimization procedures, which are essential to the protection of United States citizens and permanent residents, shall be subject to judicial review and approval. This corrects an omission in the Protect America Act which had not provided for judicial review of the adherence of minimization procedures to statutory requirements.

Section 702(f) provides that the Attorney General, in consultation with the DNI, shall adopt guidelines to ensure compliance with ***S6131** the limitations in section 702(b), including the prohibitions on the acquisition of purely domestic communications, on targeting persons within the United States, on targeting United States persons located outside the United States, and on reverse targeting. Such guidelines shall also ensure that an application for a court order is filed as required by FISA. It is intended that these guidelines will be used for training intelligence community personnel so that there are clear requirements and procedures governing the appropriate implementation of the authority under this title of FISA. The Attorney General is to provide these guidelines to the congressional intelligence committees, the judiciary committees of the House of Representatives and the Senate, and the FISA Court. Subsequent provisions implement the guidelines requirement. See section 702(g)(2)(A)(iii)(certification requirements); section 702(l)(1) and 702(l)(2) (assessment of compliance with guidelines); and section 707(b)(1)(G)(ii) (reporting on noncompliance with guidelines).

Section 702(g) requires that the Attorney General and the DNI provide to the FISA Court, prior to implementation of an authorization under subsection (a), a written certification, with any supporting affidavits. In exigent circumstances, the Attorney General and DNI may make a determination that, without immediate implementation, intelligence important to the national security will be lost or not timely acquired prior to the implementation of an authorization. In exigent circumstances, if time does not permit the submission of a certification prior to the implementation of an authorization, the certification must be submitted to the FISA Court no later than seven days after the determination is made. This seven-day time period for submission of a certification in the case of exigent circumstances is identical to the time period by which the Attorney General must apply for a court order after authorizing an emergency surveillance under other provisions of FISA, as amended by this Act.

Section 702(g)(2) sets forth the requirements that must be contained in the written certification. These elements include: that the targeting and minimization procedures have been approved by the FISA Court or will be submitted to the court with the certification; that guidelines have been adopted to ensure compliance with the limitations of subsection (b) have been adopted; that those procedures and guidelines are consistent with the Fourth Amendment; that the acquisition is targeted at persons reasonably believed to be outside the United States; that a significant purpose of the acquisition is to obtain foreign intelligence information; and an effective date for the authorization that in most cases is at least 30 days after the submission of the written certification. Additionally, as an overall limitation on the method of acquisition. permitted under section 702, the certification must attest that the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider.

Requiring an effective date in the certification serves to identify the beginning of the period of authorization (which is likely to be a year) for collection and to alert the FISA Court of when the Attorney General and DNI are seeking to begin collection. Section 702(g)(3) permits the Attorney General and DNI to change the effective date in the certification by amending the certification.

As with the Protect America Act, the certification under section 702(g)(4) is not required to identify the specific facilities, places, premises, or property at which the acquisition under section 702(a) will be directed or conducted. The certification shall be subject to review by the FISA Court.

Section 702(h) authorizes the Attorney General and the DNI to direct, in writing, an electronic communication service provider to furnish the Government with all information, facilities, or assistance necessary to accomplish the acquisition authorized under subsection 702(a). It requires compensation for this assistance and provides that no cause of action shall lie in any court against an electronic communication service provider for its assistance in accordance with a directive. Section 702(h) also establishes expedited procedures in the FISA Court for a provider to challenge the legality of a directive or the Government to enforce it. In either case, the question for the court is whether the directive meets the requirements of section 702 and is otherwise lawful. Whether the proceeding begins as a provider challenge or a Government enforcement petition, if the court upholds the directive as issued or modified, the court shall order the provider to comply. Failure to comply may be punished as a contempt of court. The proceedings shall be expedited and decided within 30 days, unless that time is extended under section 702(j)(2).

Section 702(i) provides for judicial review of any certification required by section 702(g) and the targeting and minimization procedures adopted pursuant to sections 702(d) and 702(e). In accordance with section 702(i)(5), if the Attorney General and the DNI seek to reauthorize or replace an authorization in effect under the Act, they shall submit, to the extent practicable, the certification and procedures at least 30 days prior to the expiration of such authorization.

The court shall review certifications to determine whether they contain all the required elements. It shall review targeting procedures to assess whether they are reasonably designed to ensure that the acquisition activity is limited to the targeting of persons reasonably believed to be located outside the United States and prevent the intentional acquisition of any communication whose sender and intended recipients are known to be located in the United States. The Protect America Act had limited the review of targeting procedures to a "clearly erroneous" standard; section 702(i) omits that limitation. For minimization procedures, section 702(i) provides that the court shall review them to assess whether they meet the statutory requirements. The court is to review the certifications and procedures and issue its order within 30 days after they were submitted unless that time is extended under section 702(j)(2). The Attorney General and the DNI may also amend the certification or procedures at any time under section 702(i)(1)(C), but those amended certifications or procedures must be submitted to the court in no more than 7 days after amendment. The amended procedures may be used pending the court's review.

If the FISA Court finds that the certification contains all the required elements and that the targeting and minimization procedures are consistent with the requirements of subsections (d) and (e) and with the Fourth Amendment, the court shall enter an order approving their use or continued use for the acquisition authorized by section 702(a). If it does not so find, the court shall order the Government, at its election, to correct any deficiencies or cease, or not begin, the acquisition. If acquisitions have begun, they may continue during any rehearing en banc of an order requiring the correction of deficiencies. If the Government appeals to the Foreign Intelligence Surveillance Court of Review, any collection that has begun may continue at least until that court enters an order, not later than 60 days after filing of the petition for review, which determines whether all or any part of the correction order shall be implemented during the appeal

Section 702(j)(1) provides that judicial proceedings are to be conducted as expeditiously as possible. Section 702(j)(2) provides that the time limits for judicial review in section 702 (for judicial review of certifications and procedures or in challenges or enforcement proceedings concerning directives) shall apply unless extended, by written order, as necessary for good cause in a manner consistent with national security.

Section 702(k) requires that records of proceedings under section 702 shall be maintained by the FISA Court under security measures adopted by the Chief Justice in consultation with the Attorney General and the DNI. In addition, all petitions are to be filed under seal and the FISA Court, upon the request of the Government, shall consider ex parte and in camera any Government submission or portions of a submission that may include classified information. The Attorney General and the DNI are to retain directives made or orders granted for not less than 10 years.

Section 702(l) provides for oversight of the implementation of Title VII. It has three parts. First, the Attorney General and the DNI shall assess semiannually under subsection (l)(1) compliance with the targeting and minimization procedures, and the Attorney General guidelines for compliance with limitations under section 702(b), and submit the assessment to the FISA Court and to the congressional intelligence and judiciary committees, consistent with congressional rules.

Second, under subsection (l)(2)(A), the Inspector General of the Department of Justice and the inspector general ("IG") of any intelligence community element authorized to acquire foreign intelligence under section 702(a) are authorized to review compliance of their agency or element with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f). Subsections (l)(2)(B) and (l)(2)(C) mandate several statistics that the IGs shall review with respect to United States persons, including the number of disseminated intelligence reports that contain references to particular U.S. persons, the number of U.S. persons whose identities were disseminated in response to particular requests, and the number of targets later determined to be located in the United States. Their reports shall be submitted to the Attorney General, the DNI, and the appropriate congressional committees. Section 702(l)(2) provides no statutory schedule for the completion of these IG reviews; the IGs should coordinate with the heads of their agencies about the timing for completion of the IG reviews so that they are done at a time that would be useful for the agency heads to complete their semiannual reviews.

Third, under subsection (l)(3), the head of an intelligence community element that conducts an acquisition under section 702 shall review annually whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition and provide an accounting of information pertaining to United States persons similar to that included in the IG report. Subsection (l)(3) also encourages the ***S6132** head of the element to develop procedures to assess the extent to which the new authority acquires the communications of U.S. persons, and to report the results of such assessment. The review is to be used by the head of the element to evaluate the adequacy of minimization procedures. The annual review is to be submitted to the FISA Court, the Attorney General and the DNI, and to the appropriate congressional committees.

Section 703. Certain Acquisition Inside the United States Targeting United States Persons Outside the United States

Section 703 governs the targeting of United States persons who are reasonably believed to be outside the United States when the acquisition of foreign intelligence is conducted inside the United States. The authority and procedures of section 703 apply when the acquisition either constitutes electronic surveillance, as defined in Title I of FISA, or is of stored electronic communications or stored electronic data. If the United States person returns to the United States, acquisition under section 703 must cease. The Government may always, however, obtain an order or authorization under another title of FISA.

The application procedures and provisions for a FISA Court order in sections 703(b) and 703(c) are drawn from Titles I and III of FISA. Key among them is the requirement that the FISA Court determine that there is probable cause to believe that, for the United States person who is the target of the surveillance, the person is reasonably believed to be located outside the United States and is a foreign power or an agent, officer or employee of a foreign power. The inclusion of United States persons who are officers or employees of a foreign power, as well as those who are agents of a foreign power as that term is used in FISA, is intended to permit the type of collection against United States persons outside the United States that has been allowed under existing Executive Branch guidelines. The FISA Court shall also review and approve minimization procedures that will be applicable to the acquisition, and shall order compliance with such procedures.

As with FISA orders against persons in the United States, FISA orders against United States persons outside of the United States under section 703 may not exceed 90 days and may be renewed for additional 90-day periods upon the submission of renewal applications. Emergency authorizations under section 703 are consistent with the requirements for emergency authorizations in FISA against persons in the United States, as amended by this Act; the Attorney General may authorize an emergency acquisition if an application is submitted to the FISA Court in not more than seven days.

Section 703(g) is a construction provision that clarifies that, if the Government obtains an order and target a particular United States person in accordance with section 703, FISA does not require the Government to seek a court order under any other provision of FISA to target that United States person while that person is reasonably believed to be located outside the United States.

Section 704. Other Acquisitions Targeting United States Persons Outside the United States

Section 704 governs other acquisitions that target United States persons who are outside the United States. Sections 702 and 703 address acquisitions that constitute electronic surveillance or the acquisition of stored electronic communications. In contrast, as provided in section 704(a)(2), section 704 addresses any targeting of a United States person outside of the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required if the acquisition occurred within the United States. It thus covers not only communications intelligence, but, if it were to occur, the physical search of a home, office, or business of a United States person by an element of the United States intelligence community, outside of the United States.

Pursuant to section 704(a)(3), if the targeted United States person is reasonably believed to be in the United States while an order under section 704 is in effect, the acquisition against that person shall cease unless authority is obtained under another applicable provision of FISA. Likewise, the Government may not use section 704 to authorize an acquisition of foreign intelligence inside the United States.

Section 704(b) describes the application to the FISA Court that is required. For an order under section 704(c), the FISA Court must determine that there is probable cause to believe that the United States person who is the target of the acquisition is reasonably believed to be located outside the United States and is a foreign power, or an agent, officer or employee of a foreign power. An order is valid for a period not to exceed 90 days, and may be renewed for additional 90-day periods upon submission of renewal applications meeting application requirements.

Because an acquisition under section 704 is conducted outside the United States, or is otherwise not covered by FISA, the FISA Court is expressly not given jurisdiction to review the means by which an acquisition under this section may be conducted. Although the FISA Court's review is limited to determinations of probable cause, section 704 anticipates that any acquisition conducted pursuant to a section 704 order will in all other respects be conducted in compliance with relevant regulations and Executive Orders governing the acquisition of foreign intelligence outside the United States, including Executive Order 12333 or any successor order.

Section 705. Joint Applications and Concurrent Authorizations

Section 705 provides that if an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge of the FISA Court may issue simultaneously, upon the request of the Government in a joint application meeting the requirements of sections 703 and 704, orders under both sections as appropriate. If an order authorizing electronic surveillance or physical search has been obtained under section 105 or section 304, and that order is still in effect, the Attorney General may authorize, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

Section 706. Use of Information Acquired Under Title VII

Section 706 fills a void that has existed under the Protect America Act which had contained no provision governing the use of acquired intelligence. Section 706(a) provides that information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to Title I of FISA for the purposes of section 106 of FISA, which is the provision of Title I of FISA that governs public disclosure or use in criminal proceedings. The one exception is for subsection (j) of section 106, as the notice provision in that subsection, while manageable in individual Title I proceedings, would present a difficult national security question when applied to a Title VII acquisition. Section 706(b) also provides that information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to Title I of FISA for the purposes of section 106 of FISA; however, the notice provision of subsection (j) applies. Section 706 ensures that a uniform standard for the types of information is acquired under the new title.

Section 707. Congressional Oversight

Section 707 provides for additional congressional oversight of the implementation of Title VII. The Attorney General is to fully inform "in a manner consistent with national security" the congressional intelligence and judiciary committees about implementation of the Act at least semiannually. Each report is to include any certifications made under section 702, the reasons for any determinations made under section 702(c)(2), any directives issued during the reporting period, a description of the judicial review during the reporting period to include a copy of any order or pleading that contains a significant legal interpretation of section 702, incidents of noncompliance and procedures to implement the section. With respect to sections 703 and 704, the report must contain the number of applications made for orders under each section and the number of such orders granted, modified and denied, as well as the number of emergency authorizations made pursuant to each section and the subsequent orders approving or denying the relevant application. In keeping the congressional intelligence committees fully informed, the Attorney General should provide no less information than has been provided in the past in keeping the committees fully and currently informed.

Section 708. Savings Provision

Section 708 provides that nothing in Title VII shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of FISA. This language is designed to ensure that Title VII cannot be interpreted to prevent the Government from submitting applications and seeking orders under other titles of FISA.

Section 101(b). Table of Contents

Section 101(b) of the bill amends the table of contents in the first section of FISA.

Subsection 101(c). Technical and Conforming Amendments

Section 101(c) of the bill provides for technical and conforming amendments in Title 18 of the United States Code and in FISA.

Section 102. Statement of Exclusive Means by which Electronic Surveillance and Interception of Certain Communications May Be Conducted

Section 102(a) amends Title I of FISA by adding a new Section 112 of FISA. Under the heading of "Statement of Exclusive Means by which Electronic Surveillance and Interception of Certain Communications May Be Conducted," the new section 112(a) states: "Except as provided in subsection (b), the procedures of chapters 119, 121 and 126 of Title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communication may be conducted." New section 112(b) of FISA provides that only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to FISA or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the ***S6133** purpose of subsection (a). The new section 112 is based on a provision which Congress enacted in 1978 as part of the original FISA that is codified in section 2511(2)(f) of Title 18, United States Code, and which will remain in the U.S. Code.

Section 102(a) strengthens the statutory provisions pertaining to electronic surveillance and interception of certain communications to clarify the express intent of Congress that these statutory provisions are the exclusive means for conducting electronic surveillance and interception of certain communications. With the absence of reference to the Authorization for Use of Military Force, Pub. L. 107-40, (September 18, 2001) ("AUMF"), Congress makes clear that this AUMF or any other existing statute cannot be used in the future as the statutory basis for circumventing FISA. Section 102(a) is intended to ensure that additional exclusive means for surveillance or interceptions shall be express statutory authorizations.

In accord with section 102(b) of the bill, section 109 of FISA that provides for criminal penalties for violations of FISA, is amended to implement the exclusivity requirement added in section 112 by making clear that the safe harbor to FISA's criminal offense provision is limited to statutory authorizations for electronic surveillance or the interception of domestic wire, oral, or electronic communications which are pursuant to a provision of FISA, one of the enumerated chapters of the criminal code, or a statutory authorization that expressly provides an additional exclusive means for conducting the electronic surveillance. By virtue of the cross-reference in section 110 of FISA to section 109, that limitation on the safe harbor in section 109 applies equally to section 110 on civil liability for conducting unlawful electronic surveillance.

Section 102(c) requires that when a certification for assistance to obtain foreign intelligence is based on statutory authority, the certification provided to an electronic communication service provider is to include the specific statutory authorization for the request for assistance and certify that the statutory requirements have been met. This provision is designed to assist electronic communication service providers in understanding the legal basis for any government requests for assistance.

In the section-by-section analysis of S. 2248, the report of the Select Committee on Intelligence (S. Rep. No. 110-209, at 18) described and incorporated the discussion of exclusivity in the 1978 conference report on the original Foreign Intelligence Surveillance Act, in particular the conferees' description of the Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) and the application of the principles described there to the current legislation. That full discussion should be deemed incorporated in this section-by-section analysis.

Section 103. Submittal to Congress of Certain Court Orders under the Foreign Intelligence Surveillance Act of 1978

Section 6002 of the Intelligence Reform Act and Terrorism Prevention Act of 2004 (Pub. L. 108-458), added a Title VI to FISA that augments the semiannual reporting obligations of the Attorney General to the intelligence and judiciary committees of the Senate and House of Representatives. Under section 6002, the Attorney General shall report a summary of significant legal interpretations of FISA in matters before the FISA Court or Foreign Intelligence Surveillance Court of Review. The requirement extends to interpretations presented in applications or pleadings filed with either court by the Department of Justice. In addition to the semiannual summary, the Department of Justice is required to provide copies of court decisions, but not orders, which include significant interpretations of FISA. The importance of the reporting requirement is that, because the two courts conduct their business in secret, Congress needs the reports to know how the law it has enacted is being interpreted.

Section 103 improves the Title VI reporting requirements in three ways. First, as significant legal interpretations may be included in orders as well as opinions, section 103 requires that orders also be provided to the committees. Second, as the semiannual report often takes many months after the end of the semiannual period to prepare, section 103 accelerates provision of information about significant legal interpretations by requiring the submission of such decisions, orders, or opinions within 45 days. Finally, section 103 requires that the Attorney General shall submit a copy of any such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, from the period five years preceding enactment of the bill that has not previously been submitted to the congressional intelligence and judiciary committees.

OVERVIEW OF SECTIONS 104 THROUGH SECTION 109. FISA STREAMLINING

Sections 104 through 109 amend various sections of FISA for such purposes as reducing a paperwork requirement, modifying time requirements, or providing additional flexibility in terms of the range of Government officials who may authorize FISA actions. Collectively, these amendments are described as streamlining amendments. In general, they are intended to increase the efficiency of the FISA process without depriving the FISA Court of the information it needs to make findings required under FISA.

Section 104. Applications for Court Orders

Section 104 of the bill strikes two of the eleven paragraphs on standard information in an application for a surveillance order under section 104 of FISA, either because the information is provided elsewhere in the application process or is not needed.

In various places, FISA has required the submission of "detailed" information, as in section 104 of FISA, "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance." The DNI requested legislation that asked that " summary" be substituted for "detailed" for this and other application requirements, in order to reduce the length of FISA applications. In general, the bill approaches this by eliminating the mandate for "detailed" descriptions, leaving it to the FISA Court and the Government to work out the level of specificity needed by the FISA Court to perform its statutory responsibilities. With respect to one item of information, "a statement of the means by which the surveillance will be effected," the bill modifies the requirement by allowing for "a summary statement."

In aid of flexibility, section 104 increases the number of individuals who may make FISA applications by allowing the President to designate the Deputy Director of the Federal Bureau of Investigation ("FBI") as one of those individuals. This should enable the Government to move more expeditiously to obtain certifications when the Director of the FBI is away from Washington or otherwise unavailable.

Subsection (b) of section 104 of FISA is eliminated as obsolete in light of current applications. The Director of the Central Intelligence Agency is added to the list of officials who may make a written request to the Attorney General to personally review a FISA application as the head of the CIA had this authority prior to the establishment of the Office of the Director of National Intelligence.

Section 105. Issuance of an Order

Section 105 strikes from Section 105 of FISA several unnecessary or obsolete provisions. Section 105 strikes subsection (c)(1)(F) of Section 105 of FISA which requires minimization procedures applicable to each surveillance device employed because Section 105(c)(2)(A) requires each order approving electronic surveillance to direct the minimization procedures to be followed.

Subsection (a)(6) reorganizes, in more readable form, the emergency surveillance provision of section 105(f), now redesignated section 105(e), with a substantive change of extending from 3 to 7 days the time by which the Attorney General must apply for and obtain a court order after authorizing an emergency surveillance. The purpose of the change is to help make emergency authority a more practical tool while keeping it within the parameters of FISA.

Subsection (a)(7) adds a new paragraph to section 105 of FISA to require the FISA Court, on the Government's request, when granting an application for electronic surveillance, to authorize at the same time the installation and use of pen registers and trap and trace devices. This will save the paperwork that had been involved in making two applications.

Section 106. Use of Information

Section 106 amends section 106(i) of FISA with regard to the limitations on the use of unintentionally acquired information. Currently, section 106(i) of FISA provides that unintentionally acquired radio communication between persons located in the United States must be destroyed unless the Attorney General determines that the contents of the communications indicates a threat of death or serious bodily harm to any person. Section 106 of the bill amends subsection 106(i) of FISA by making it technology neutral on the principle that the same rule for the use of information indicating threats of death or serious harm should apply no matter how the communication is transmitted.

Section 107. Amendments for Physical Searches

Section 107 makes changes to Title III of FISA: changing applications and orders for physical searches to correspond to changes in sections 104 and 105 on reduction of some application paperwork; providing the FBI with administrative flexibility in enabling its Deputy Director to be a certifying officer; and extending the time, from 3 days to 7 days, for applying for and obtaining a court order after authorization of an emergency search.

Section 303(a)(4)(C), which will be redesignated section 303(a)(3)(C), requires that each application for physical search authority state the applicant's belief that the property is "owned, used, possessed by, or is in transmit to or from" a foreign power or an agent of a foreign power. In order to provide needed flexibility and to make the provision consistent with electronic surveillance provisions, section 107(a)(1)(D) of the bill allows the FBI to apply for authority to search property that also is "about to be" owned, used, or possessed by a foreign power or agent of a foreign power, or in transit to or from one.

Section 108. Amendments for Emergency Pen Registers and Trap and Trace Devices

Section 108 amends section 403 of FISA to extend from 2 days to 7 days the time for applying for and obtaining a court order after an emergency installation of a pen register or trap and trace device. This change harmonizes among FISA's provisions for electronic surveillance, search, and pen register/***S6134** trap and trace authority the time requirements that follow the Attorney General's decision to take emergency action.

Section 109. Foreign Intelligence Surveillance Court

Section 109 contains four amendments to section 103 of FISA, which establishes the FISA Court and the Foreign Intelligence Surveillance Court of Review.

Section 109(a) amends section 103 to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement-that the eleven judges be drawn from seven judicial circuits (with the number appearing to be a ceiling rather than a floor) has proven unnecessarily restrictive or complicated for the designation of the judges to the FISA Court.

Section 109(b) amends section 103 to allow the FISA Court to hold a hearing or rehearing of a matter en banc, which is by all the judges who constitute the FISA Court sitting together. The Court may determine to do this on its own initiative, at the request of the Government in any proceeding under FISA, or at the request of a party in the few proceedings in which a private entity or person may be a party, i.e., challenges to document production orders under Title V, or proceedings on the legality or enforcement of directives to electronic communication service providers under Title VII.

Under section 109(b), en banc review may be ordered by a majority of the judges who constitute the FISA Court upon a determination that it is necessary to secure or maintain uniformity of the court's decisions or that a particular proceeding involves a question of exceptional importance. En banc proceedings should be rare and in the interest of the general objective of fostering expeditious consideration of matters before the FISA Court.

Section 109(c) provides authority for the entry of stays, or the entry of orders modifying orders entered by the FISA Court or the Foreign Intelligence Surveillance Court of Review, pending appeal or review in the Supreme Court. This authority is supplemental to, and does not supersede, the specific provision in section 702(i)(4)(B) that acquisitions under Title VII may continue during the pendency of any rehearing en banc and appeal to the Court of Review subject to the requirement for a determination within 60 days under section 702(i)(4)(C).

Section 109(d) provides that nothing in FISA shall be construed to reduce or contravene the inherent authority of the FISA Court to determine or enforce compliance with any order of that court or with a procedure approved by it.

Section 110. Weapons of Mass Destruction

Section 110 amends the definitions in FISA of foreign power and agent of a foreign power to include individuals who are not United States persons and entities not substantially composed of United States persons that are engaged in the international proliferation of weapons of mass destruction. Section 110 also adds a definition of weapon of mass destruction to the Act that defines weapons of mass destruction to cover explosive, incendiary, or poison gas devices that are designed, intended to, or have the capability to cause a mass casualty incident or death, and biological, chemical and nuclear weapons that are designed, intended to, or have the capability to cause illness or serious bodily injury to a significant number of persons. Section 110 also makes corresponding, technical and conforming changes to FISA.

Title II. Protections for Electronic Communication Service Providers

This title establishes a new Title VIII of FISA. The title addresses liability relief for electronic communication service providers who have been alleged in various civil actions to have assisted the U.S. Government between September 11, 2001, and January 17, 2007, when the Attorney General announced the termination of the Terrorist Surveillance Program. In addition, Title VIII contains provisions of law intended to implement statutory defenses for electronic communication service providers and others who assist the Government in accordance with precise, existing legal requirements, and for providing for federal preemption of state investigations. The liability protection provisions of Title VIII are not subject to sunset.

Section 801. Definitions

Section 801 establishes definitions for Title VIII. Several are of particular importance.

The term "assistance" is defined to mean the provision of, or the provision of access to, information, facilities, or another form of assistance. The word "information" is itself described in a parenthetical to include communication contents, communication records, or other information relating to a customer or communications. "Contents" is defined by reference to its meaning in Title I of FISA. By that reference, it includes any information concerning the identity of the parties to a communication or the existence, substance, purport, or meaning of it.

The term "civil action" is defined to include a "covered civil action." Thus, "covered civil actions" are a subset of civil actions, and everything in new Title VIII that is applicable generally to civil actions is also applicable to "covered civil actions." A "covered civil action" has two key elements. It is defined as a civil action filed in a federal or state court which (1) alleges that an electronic communication service provider (a defined term) furnished assistance to an element of the intelligence community and (2) seeks monetary or other relief from the electronic communication service provider related to the provision of the assistance. Both elements must be present for the lawsuit to be a covered civil action.

The term "person" (the full universe of those protected by section 802) is necessarily broader than the definition of electronic communication service provider. The aspects of Title VIII that apply to those who assist the Government in accordance with precise, existing legal requirements apply to all who may be ordered to provide assistance under FISA, such as custodians of records who may be directed to produce records by the FISA Court under Title V of FISA or landlords who may be required to provide access under Title I or III of FISA, not just to electronic communication service providers.

Section 802. Procedures for Implementing Statutory Defenses

Section 802 establishes procedures for implementing statutory defenses. Notwithstanding any other provision of law, no civil action may lie or be maintained in a federal or state court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General makes a certification to the district court in which the action is pending. (If an action had been commenced in state court, it would have to be removed, pursuant to section 802(g) to a district court, where a certification under section 802 could be filed.) The certification must state either that the assistance was not provided (section 802(a)(5)) or, if furnished, that it was provided pursuant to specific statutory requirements (sections 802(a)(1-4)). Three of these underlying requirements, which are specifically described in section 802 (sections 802(a)(1-3)), come from existing law. They include: an order of the FISA Court directing assistance, a certification in writing under sections 2511(2)(a)(ii)(B) or 2709(b) of Title 18, or directives to electronic communication service providers under particular sections of FISA or the Protect America Act.

The Attorney General may only make a certification under the fourth statutory requirement, section 802(a)(4), if the civil action is a covered civil action (as defined in section 801(5)). To satisfy the requirements of section 802(a)(4), the Attorney General must certify first that the assistance alleged to have been provided by the electronic communication service provider was in connection with an intelligence activity involving communications that was (1) authorized by the President between September 11, 2001 and January 17, 2007 and (2) designed to detect or prevent a terrorist attack or preparations for one against the United States. In addition, the Attorney General must also certify that the assistance was the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head (or deputy to the head) of an element of the intelligence community to the electronic communication service provider indicating that the activity was (1) authorized by the President and (2) determined to be lawful. The report of the Select Committee on Intelligence contained a description of the relevant correspondence provided to electronic communication service providers (S. Rep. No. 110-209, at 9).

The district court must give effect to the Attorney General's certification unless the court finds it is not supported by substantial evidence provided to the court pursuant to this section. In its review, the court may examine any relevant court order, certification, written request or directive submitted by the Attorney General pursuant to subsection (b)(2) or by the parties pursuant to subsection (d). Section 802 is silent on the nature of any additional materials that the Attorney General may submit beyond those listed in subsection (b)(2) if the Attorney General determines they are necessary to provide substantial evidence to support the certification, such as if the Attorney General certifies that a person did not provide the alleged assistance.

If the Attorney General files a declaration that disclosure of a certification or supplemental materials would harm national security, the court shall review the certification and supplemental materials in camera and ex parte, which means with only the Government present. A public order following that review shall be limited to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the basis for the certification of the Attorney General. The purpose of this requirement is to protect the classified national security information involved in the identification of providers who assist the Government. A public order shall not disclose whether the certification was based on an order, certification, or directive, or on the ground that the electronic communication service provider furnished no assistance. Because the district court must find that the certification-including a certification that states that a party did not provide the alleged assistance-is supported by substantial evidence in order to dismiss a case, an order failing to dismiss a case is only a conclusion that the substantial evidence test has not been met. It does not indicate whether a particular provider assisted the government.

Subsection (d) makes clear that any plaintiff or defendant in a civil action may submit any relevant court order, certification, written request, or directive to the district court for review and be permitted to participate in the briefing or argument of any legal ***S6135** issue in a judicial proceeding conducted pursuant to this section, to the extent that such participation does not require the disclosure of classified information to such party. The authorities of the Attorney General under section 802 are to be performed only by the Attorney General, the Acting Attorney General, or the Deputy Attorney General.

In adopting the portions of section 802 that allow for liability protection for those electronic communication service providers who may have participated in the program of intelligence activity involving communications authorized by the President between September 11, 2001, and January 17, 2007, the Congress makes no statement on the legality of the program. This is in accord with the statement in the report of the Senate Intelligence Committee that "Section 202 <as the immunity provision was then numbered> makes no assessment about the legality of the President's program." S. Rep. No. 110-209, at 9.

Section 803. Preemption of State Investigations

Section 803 addresses actions taken by a number of state regulatory commissions to force disclosure of information concerning cooperation by state regulated electronic communication service providers with U.S. intelligence agencies. Section 803 preempts these state actions and authorizes the United States to bring suit to enforce the prohibition.

Section 804. Reporting

Section 804 provides for oversight of the implementation of Title VIII. On a semiannual basis, the Attorney General is to provide to the appropriate congressional committees a report on any certifications made under section 802, a description of the judicial review of the certifications made under section 802, and any actions taken to enforce the provisions of section 803.

Section 202. Technical Amendments

Section 202 amends the table of contents of the first section of FISA.

TITLE III. REVIEW OF PREVIOUS ACTIONS

Title III directs the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the Department of Defense, the National Security Agency, and any other element of the intelligence community that participated in the President's surveillance program, defined in the title to mean the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, to complete a comprehensive review of the program with respect to the oversight authority and responsibility of each such inspector general.

The review is to include: all of the facts necessary to describe the establishment, implementation, product, and use of the product of the program; access to legal reviews of the program and information about the program; communications with, and participation of, individuals and entities in the private sector related to the program; interaction with the FISA Court and transition to court orders related to the program; and any other matters identified by any such inspector general that would enable that inspector general complete a review of the program with respect to the inspector general's department or element.

The inspectors general are directed to work in conjunction, to the extent practicable, with other inspectors general required to conduct a review, and not unnecessarily duplicate or delay any reviews or audits that have already been completed or are being undertaken with respect to the program. In addition, the Counsel of the Office of Professional Responsibility of the Department of Justice is directed to provide the report of any investigation of that office relating to the program, including any investigation of the process through which the legal reviews of the program were conducted and the substance of such reviews, to the Inspector General of the Department of Justice, who shall integrate the factual findings and conclusions of such investigation into its review.

The inspectors general shall designate one of the Senate confirmed inspectors general required to conduct a review to coordinate the conduct of the reviews and the preparation of the reports. The inspectors general are to submit an interim report within sixty days to the appropriate congressional committees on their planned scope of review. The final report is to be completed no later than one year after enactment and shall be submitted in unclassified form, but may include a classified annex.

The Congress is aware that the Inspector General of the Department of Justice has undertaken a review of the program. This review should serve as a significant part of the basis for meeting the requirements of this title. In no event is this title intended to delay or duplicate the investigation completed to date or the issuance of any report by the Inspector General of the Department of Justice.

TITLE IV. OTHER PROVISIONS

Section 401. Severability

Section 401 provides that if any provision of this bill or its application is held invalid, the validity of the remainder of the Act and its application to other persons or circumstances is unaffected.

Section 402. Effective Date

Section 402 provides that except as provided in the transition procedures (section 404 of the title), the amendments made by the bill shall take effect immediately.

Section 403. Repeals

Section 403(a) provides for the repeal of those sections of FISA enacted as amendments to FISA by the Protect America Act, except as provided otherwise in the transition procedures of section 404, and makes technical and conforming amendments.

Section 403(b) provides for the sunset of the FISA Amendments Act on December 31, 2012, except as provided in section 404 of the bill. This date ensures that the amendments by the Act will be reviewed during the next presidential administration. The subsection also makes technical and conforming amendments.

Section 404. Transition Procedures

Section 404 establishes transition procedures for the Protect America Act and the Foreign Intelligence Surveillance Act Amendments of 2008.

Subsection (a)(1) continues in effect orders, authorizations, and directives issued under FISA, as amended by section 2 of the Protect America Act, until the expiration of such order, authorization or directive.

Subsection (a)(2) sets forth the provisions of FISA and the Protect America Act that continue to apply to any acquisition conducted under such Protect America Act order, authorization or directive. In addition, subsection (a) clarifies the following provisions of the Protect America Act: the protection from liability provision of subsection (l) of Section 105B of FISA as added by section 2 of the Protect America Act; jurisdiction of the FISA Court with respect to a directive issued pursuant to the Protect America Act, and the Protect America Act reporting requirements of the Attorney General and the DNI. Subsection (a) is made effective as of the date of enactment of the Protect America Act (August 5, 2007). The purpose of these clarifications and the effective date for them is to ensure that there are no gaps in the legal protections contained in that act, including for authorized collection following the sunset of the Protect America Act, notwithstanding that its sunset provision was only extended once until February 16, 2008. Additionally, subsection (a)(3) fills a void in the Protect America Act and applies the use provisions of section 106 of FISA to collection under the Protect America Act, in the same manner that section 706 does for collection under Title VII.

In addition, subsection (a)(7) makes clear that if the Attorney General and the DNI seek to replace an authorization made pursuant to the Protect America Act with an authorization made under section 702, as added by this bill, they are, to the extent practicable, to submit a certification to the FISA Court at least 30 days in advance of the expiration of such authorization. The authorizations, and any directives issued pursuant to the authorization, are to remain in effect until the FISA Court issues an order with respect to that certification.

Subsection (b) provides similar treatment for any order of the FISA Court issued under Title VII of this bill in effect on December 31, 2012.

Subsection (c) provides transition procedures for the authorizations in effect under section 2.5 of Executive Order 12333. Those authorizations shall continue in effect until the earlier of the date that authorization expires or the date that is 90 days after the enactment of this Act. This transition provision is particularly applicable to the transition to FISA Court orders that will occur as a result of sections 703 and 704 of FISA, as added by this bill.